iSR6142
Router Manager

User's Guide

SN0054660-00 A

Information furnished in this manual is believed to be accurate and reliable. However, QLogic Corporation assumes no responsibility for its use, nor for any infringements of patents or other rights of third parties which may result from its use. QLogic Corporation reserves the right to change product specifications at any time without notice. Applications described in this document for any of these products are for illustrative purposes only. QLogic Corporation makes no representation nor warranty that such applications are suitable for the specified use without further testing or modification. QLogic Corporation assumes no responsibility for any errors that may appear in this document.

QLogic is a registered trademark and SmartWrite is a trademark of QLogic Corporation.

AMCC is a registered trademark of Applied Micro Circuits Corporation

Brocade is a registered trademark of Brocade Communications Systems, Inc.

Cisco is a registered trademark of Cisco Technology, Inc.

Gnome is a trademark of the GNOME Foundation Corporation.

Java and Solaris are registered trademarks of Sun Microsystems, Inc.

Pentium is a registered trademark of Intel Corporation.

IBM and PowerPC are registered trademarks of the International Business Machines Corporation.

Linux is a registered trademark of Linus Torvalds.

MacOS X and Safari are registered trademarks of Apple Computer, Inc.

McDATA is a registered trademark of McDATA Corporation.

Microsoft, Windows XP, Windows 2003, and Internet Explorer are registered trademarks of Microsoft Corporation.

Netscape Navigator and Mozilla are trademarks or registered trademarks of Netscape Communications Corporation.

Red Hat is a registered trademark of Red Hat Software Inc.

SANmark is a trademark of the Fibre Channel Industry Association.

SUSE is a trademark of Novell, Inc.

All other brand and product names are trademarks or registered trademarks of their respective owners.

Document Revision History

Revision A

Changes	Sections Affected
New document	

© 2008 QLogic Corporation. All Rights Reserved Worldwide.
Published: September 2008

QLogic Corporation, 26650 Aliso Viejo Parkway, Aliso Viejo, CA 92656, (800) 662-4471 or (949) 389-6000

Table of Contents

1 Introduction

Intended Audience 1-1
Related Materials 1-1
Technical Support 1-2
Availability 1-2
Training 1-3
Contact Information 1-3

2 Using the Graphical User Interface (GUI)

Main Window 2-2
Menu Bar 2-3
File Menu 2-4
View Menu 2-4
Settings Menu 2-4
Wizards Menu 2-5
Help Menu 2-7
Tool Bar 2-7
Action Menu 2-8
System Tree Window 2-10

3 Managing the Router

iSR6142 Router 3-1
Information Tab 3-2
Basic Information 3-2
Management Information 3-3
NTP Server Information 3-5
Security 3-6
SNMP Management Tab 3-7
SNMP Configuration 3-7
SNMP Trap Receivers 3-8
Features Tab 3-9
Assigned Remote Router Tab 3-9
Topology Tab 3-10

FC Ports 3-11
FC Port Information Tab 3-11
FC Port Advanced Configuration Tab 3-12
FC Port Performance Tab 3-13
iSCSI Ports 3-14
Information Tab 3-14
iSCSI Port Information 3-15
iSCSI Port Network Settings 3-16
Advanced Configuration Tab 3-18
Statistics Tab 3-21
Discovered iSCSI Initiators 3-22
Information Tab 3-22
Local Presented Target Tab 3-23
Remote Presented Target Tab 3-24
FC Discovered Targets 3-25
Information Tab 3-26
Remote Presented Devices Tab 3-26
iSCSI Presented Target List Tabbed Page 3-27
iSCSI Discovered Targets 3-29
Information Tabbed Page 3-29
FCIP Routes 3-30
FCIP Route Information Tabbed Page 3-31
FCIP Route Statistics Tabbed Page 3-33

4 Using the Wizards

Launching a Wizard 4-1
Configuration Wizard 4-2
Add Initiator Wizard 4-7
FW Update Wizard 4-9
Map Local Initiator/Target Wizard 4-13
Unmap Local Initiator/Target Wizard 4-20
Add Remote Router Wizard 4-25
Remove Remote Router Wizard 4-30
Map Remote Initiator/Target Wizard 4-33
Unmap Remote Initiator/Target Wizard 4-40
Discover iSCSI Target Wizard 4-42
FCIP Route Add Wizard 4-45
FCIP Route Remove Wizard 4-51

5 Configuring CHAP

CHAP Definition 5-1
Discovery Session—Bi-directional CHAP 5-2
Discovery Session—Uni-directional CHAP 5-3
Normal Session—Bi-directional CHAP 5-3
Normal Session—Uni-directional CHAP 5-4

A Log Messages

Log Data A-1
Informational Log Messages A-1
Application Modules A-2
iSCSI Driver A-4
Fibre Channel Driver A-5
User Modules A-6
FCIP A-8
TOE Driver A-9
System A-9
Error Log Messages A-10
Application Modules A-10
iSCSI Driver A-18
Fibre Channel Driver A-20
User Modules A-22
System A-25
Fatal Log Messages A-25
iSCSI Driver A-25
FC Driver A-28
TOE Driver A-30
System A-31

B Simple Network Management Protocol (SNMP)

Introduction B-1
SNMP Properties B-1
SNMP Trap Configuration B-2
Management Information Base (MIB) B-3
System Information B-3
Network Port Table B-4
Fibre Channel Port Table B-6
Sensor Table B-8

Notifications B-11
Notification Objects B-11
Agent Start Up Notification B-12
Agent Shut Down Notification B-12
Network Port Down Notification B-12
Fibre Channel Port Down Notification B-12
Sensor Notification B-13
Generic Notification B-13

List of Figures

Figure		Page
2-1	SANsurfer Router Manager Main Window	2-2
2-2	Menu Bar	2-3
2-3	File Menu	2-4
2-4	View Menu	2-4
2-5	Settings Menu	2-4
2-6	Broadcast Settings Menu	2-5
2-7	Wizards Menu	2-5
2-8	Help Menu	2-7
2-9	Tool Bar	2-7
2-10	Action Menu	2-8
2-11	System Tree Window	2-10
2-12	Component Information	2-11
3-1	Basic Information Vertical Tab	3-2
3-2	Management Information Vertical Tab	3-3
3-3	NTP Server Information Vertical Tab	3-5
3-4	Security Vertical Tab	3-6
3-5	SNMP Management Tabbed Page	3-7
3-6	Features Tabbed Page	3-9
3-7	Topology Tabbed Page	3-10
3-8	FC Port Information Tab	3-11
3-9	FC Port Advanced Configuration Tab	3-12
3-10	FC Port Performance Tab	3-13
3-11	iSCSI Port Tabbed Pages	3-14
3-12	Advanced Configuration Tabbed Page	3-18
3-13	iSCSI Statistics Tabbed Page	3-21
3-14	Discovered iSCSI Initiator Tabbed Pages	3-22
3-15	Local Presented Target Tabbed Page	3-23
3-16	Remote Presented Target Tabbed Page	3-24
3-17	FC Discovered Targets Tabbed Pages	3-25
3-18	Remote Presented Devices Tab	3-26
3-19	iSCSI Presented Target List Tabbed Page	3-27
3-20	iSCSI Discovered Targets Tabbed Pages	3-29
3-21	FCIP Route Tabbed Pages	3-30

3-22 FCIP Route Statistics Page . . . 3-33
4-1 iSCSI Port Selection Dialog Box . . . 4-2
4-2 iSCSI Port Connection Settings Panel Dialog Box. . . . 4-3
4-3 iSCSI Port IPv6 Settings Panel . . . 4-4
4-4 Confirm Changes Dialog Box. . . . 4-5
4-5 iSCSI Port Configuration Status . . . 4-6
4-6 Configuration Wizard Finish Dialog Box. . . . 4-7
4-7 Create an Initiator Dialog Box . . . 4-8
4-8 Security Check Dialog Box. . . . 4-8
4-9 System Tree with New iSCSI Initiator . . . 4-9
4-10 Router Selection Dialog Box . . . 4-9
4-11 Firmware File Selection Dialog Box . . . 4-10
4-12 Confirm Changes Dialog Box. . . . 4-11
4-13 Security Check Dialog Box. . . . 4-11
4-14 Firmware Update Status Dialog Box—Progress . . . 4-12
4-15 Finish Dialog Box (Successful Firmware Update) . . . 4-12
4-16 Initiator Selection Dialog Box . . . 4-13
4-17 Select a Target Dialog Box. . . . 4-14
4-18 Select Initiator Port Dialog Box . . . 4-15
4-19 Select Target Presentation Port Dialog Box . . . 4-16
4-20 Confirm Changes Dialog Box. . . . 4-17
4-21 Security Check Dialog Box. . . . 4-18
4-22 Initiator/Target Mapping Configuration Status Dialog Box . . . 4-19
4-23 Discovered iSCSI Initiators - Local Presented Targets . . . 4-20
4-24 Initiator Selection Dialog Box . . . 4-21
4-25 Presented Target Selection Dialog Box . . . 4-22
4-26 Security Check Dialog Box. . . . 4-23
4-27 Unpresent Initiator/Target Status Dialog Box . . . 4-24
4-28 Discovered iSCSI Initiators - Local Presented Targets . . . 4-25
4-29 Remote Router's IP Address Dialog Box . . . 4-26
4-30 Local Router Admin Password Dialog Box . . . 4-27
4-31 Add Remote Router Status Dialog Box . . . 4-27
4-32 Assigned Remote Router Display . . . 4-28
4-33 Topology Display . . . 4-29
4-34 Select Remote Router Dialog Box . . . 4-30
4-35 Local Router Admin Password Dialog Box . . . 4-31
4-36 Refresh Screen . . . 4-31
4-37 Remove Remote Router Completion Dialog Box. . . . 4-32
4-38 Device Selection Dialog Box . . . 4-33
4-39 Device Selection Dialog Box . . . 4-34
4-40 Port Selection Dialog Box . . . 4-35
4-41 Device Mapping Option Dialog Box . . . 4-36
4-42 Confirm Mapping Dialog Box . . . 4-37
4-43 Local Password Dialog Box . . . 4-37
4-44 Local Router Admin Password Dialog Box . . . 4-38

4-45 Refresh Screen 4-38
4-46 Remote Mapped Device. 4-39
4-47 Device Selection Dialog Box 4-40
4-48 Local Router Admin Password Dialog Box 4-41
4-49 Remote Unmap Initiator-Target Status Dialog Box. 4-41
4-50 Discover iSCSI Target Wizard—IP Address Dialog Box 4-42
4-51 Discover iSCSI Target Wizard—Security Check Dialog Box. 4-43
4-52 Discover iSCSI Target Wizard—Refresh Dialog Box. 4-43
4-53 iSCSI Discovered Targets 4-44
4-54 FCIP Route Add Wizard—Warning Dialog Box. 4-45
4-55 FCIP Route Add Wizard—Port Selection Dialog Box 4-46
4-56 FCIP Route Add Wizard—Local and Remote IP Address Dialog Box 4-47
4-57 FCIP Route Add Wizard—TCP/IP Options Dialog Box 4-48
4-58 FCIP Route Add Wizard—FCIP Options Dialog Box. 4-49
4-59 FCIP Route Add Wizard—Security Check Dialog Box 4-50
4-60 FCIP Route Add Wizard—Completed Dialog Box. 4-50
4-61 FCIP Route Remove Wizard—Warning Dialog Box 4-51
4-62 FCIP Route Remove Wizard—Route Selection Dialog Box 4-52
4-63 FCIP Route Remove Wizard—Security Check Dialog Box. 4-52
4-64 FCIP Route Remove Wizard—Completed Dialog Box 4-53

List of Tables

Table **Page**

2-1 SANsurfer Router Manager Main Window Sections 2-2
A-1 Application Modules—Informational Log Messages A-2
A-2 iSCSI Driver—Informational Log Messages A-4
A-3 Fibre Channel Driver—Informational Log Messages. A-5
A-4 User Modules—Informational Log Messages A-6
A-5 FCIP—Informational Log Messages A-8
A-6 TOE—Informational Log Messages. A-9
A-7 System—Informational Log Messages A-9
A-8 Application Module—Error Log Messages A-10
A-9 iSCSI Driver—Error Log Messages. A-18
A-10 Fibre Channel Driver—Error Log Messages A-20
A-11 User Modules—Error Log Messages A-22
A-12 System—Error Log Messages. A-25
A-13 iSCSI Driver—Fatal Log Messages. A-25
A-14 Fibre Channel Driver—Fatal Log Messages A-28
A-15 TOE—Fatal Log Messages A-30
A-16 System—Fatal Log Messages. A-31
B-1 SNMP Properties B-1
B-2 SNMP Trap Configuration Parameters. B-2

1 Introduction

This manual describes the features of the SANsurfer Router Manager used to configure and manage the QLogic iSR6142 Intelligent Storage Router (iSR-6142).

For hardware installation, configuration, and diagnostic details, see the *iSR6142 Router Installation Guide*.

Intended Audience

This guide is for users who are responsible for installing, managing, and servicing the iSR6142 router and the storage area network (SAN) equipment to which it is attached.

Related Materials

- *iSR6142 Router Installation Guide*, part number SN0051102-00
- *iSR6142 Router CLI User's Guide*, part number SN0054659-00
- *Internet Protocol, Version 6 (IPv6) Specification*, RFC2460
- *Neighbor Discovery for IP Version 6 (IPv6),* RFC2461
- *IPv6 Stateless Address Autoconfiguration*, RFC2462
- *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*, RFC2463
- *Transmission of IPv6 Packets over Ethernet Networks*, RFC2464 iSCSI draft standard draft-ietf-ips-iSCSI-20
- *Internet engineering task force (IETF) – iSCSI Requirements and Design Considerations, iSCSI Naming and Discovery, Internet Protocol Specification (IPv4)*, RFC793
- *Transmission Control Protocol (TCP) Specification,* RFC1122, Requirements for Internet Hosts-Communication Layers
- *TCP Extensions for High Performance*, RFC1323
- *TCP Congestion Control*, RFC2581
- *NewReno Modification to TCP's Fast Recovery Algorithm*, RFC2582

- *ANSI SCSI – SCSI-3 Architecture Model (SAM), X3T10/994D/Rev 18, SCSI-3 Controller Command Set, X3T10/Project 1047D/Rev 6c. IEEE – 802.1Q Virtual LAN (VLAN), 802.1p Priority of Service, 802.3x Flow Control, 802.3ad Link Aggregation*
- *SCSI-3 Fibre Channel Protocol (SCSI-FCP)*, X3.269:1996
- *Fibre Channel Physical and Signaling Interface (FC-PH)*, X3.230:199
- *Fibre Channel 2nd Generation (FC-PH-2)*, X3.297:1997
- *Third Generation Fibre Channel Physical and Signaling Interface (FC-PH-3), X3.303:1998, Fibre Channel-Arbitrated Loop (FC-AL-2)*, working draft, revision 6.4, August 28, 1998
- *Fibre Channel Fabric Loop Attachment Technical Report (FC-FLA) NCITS/TR-20:1998, Fibre Channel-Private Loop Direct Attach Technical Report (FC-PLDA)*
- *SCSI Fibre Channel Protocol-2 (FCP-2)* working draft, revision 3, October1, 1999
- *Fibre Channel over TCP/IP (FCIP)*, RFC3821
- *ANSI Information Technology-SCSI 3 Architecture Model*, revision 18, November 27, 1995

Technical Support

Customers should contact their authorized maintenance provider for technical support of their QLogic products. QLogic-direct customers may contact QLogic Technical Support; others will be redirected to their authorized maintenance provider.

Visit the QLogic support Web site listed in Contact Information for the latest firmware and software updates.

Availability

QLogic Technical Support for products under warranty is available during local standard working hours excluding QLogic Observed Holidays.

Training

QLogic offers certification training for the technical professional for QLogic HBAs, CNAs, switches, and routers. From the training link at www.qlogic.com, you may choose Electronic-Based Training or schedule an intensive "hands-on" Certification course.

Technical Certification courses include installation, maintenance and troubleshooting QLogic SAN products. Upon demonstrating knowledge using live equipment, QLogic awards a certificate identifying the student as a Certified Professional. The training professionals at QLogic may be reached by email at tech.training@qlogic.com.

Contact Information

Support Headquarters	QLogic Corporation 4601 Dean Lakes Blvd Shakopee, MN 55379 USA
QLogic Web Site	www.qlogic.com
Technical Support Web Site	support.qlogic.com
Technical Support Email	support@qlogic.com
Technical Training Email	tech.training@qlogic.com
North American Region	
Email	support@qlogic.com
Phone	+1-952-952-4040
Fax	+1-952-687-2504
Europe, Middle East, and Africa Region	
Email	emeasupport@qlogic.com
Phone Numbers by Language	+353 1 6924960 - English +353 1 6924961 - Français +353 1 6924962 - Deutsch +353 1 6924963 - Español +353 1 6924964 - Português +353 1 6924965 - Italiano
Asia Pacific Region	
Email	apacsupport@qlogic.com

Phone Numbers by Language	+63-2-885-6712 - English +63-2-885-6713 - (Mandarin) +63-2-885-6714 - (Japanese) +63-2-885-6715 - (Korean)
Latin and South America Region	
Email	calasupport@qlogic.com
Phone Numbers by Language	+52 55 5278 7016 - English +52 55 5278 7017 - Español +52 55 5278 7015 - Português

2 Using the Graphical User Interface (GUI)

The iSR6142 management application is a graphical user interface (GUI) consisting of menus, buttons, and windows that you can use to manage iSR6142s from a workstation on Linux® and Windows® platforms. You can view and change network, port, security, and mapping configuration for one or more iSR6142s. The application displays the most current system information.

The following sections describe the GUI components:

- "Main Window" on page 2-2
- "Menu Bar" on page 2-3
- "Tool Bar" on page 2-7
- "Action Menu" on page 2-8
- "System Tree Window" on page 2-10

Main Window

The SANsurfer Router Manager consists of a menu bar, a tool bar, a system tree, and information/status/data windows and tabs, as illustrated in Figure 2-1 and described in Table 2-1.

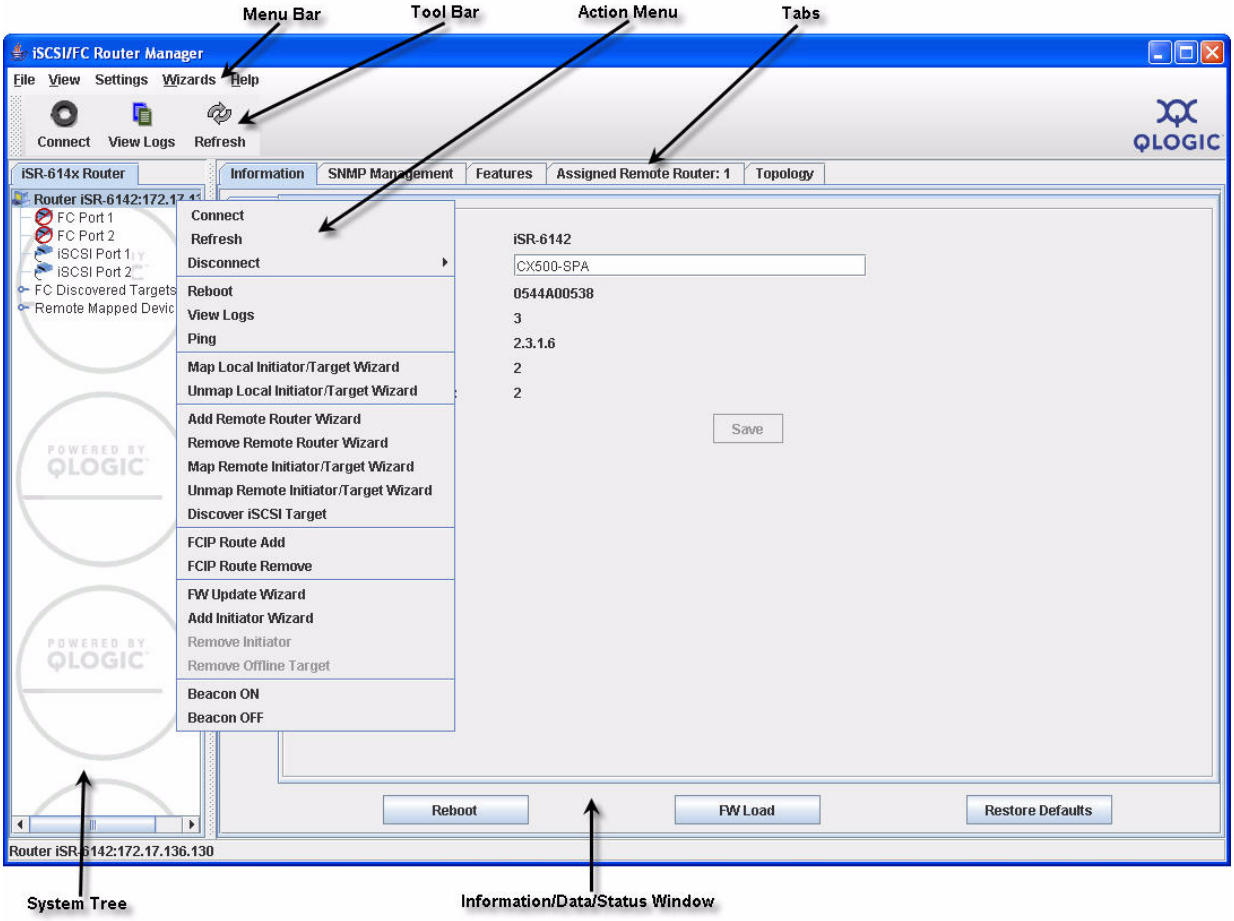

Figure 2-1 SANsurfer Router Manager Main Window

Table 2-1. SANsurfer Router Manager Main Window Sections

Item	Description
Menu Bar	The menu bar provides access to system functions and wizards.
Tool Bar	The tool bar buttons provide quick access to the common application functions: **Connect**, **View Logs**, and **Refresh**.

Table 2-1. SANsurfer Router Manager Main Window Sections (Continued)

Item	Description
System Tree	Located on the on the left side of the display, the system tree shows the connected systems and their components. An entry handle located to the left of an entry in the tree shows that you can expand that entry. Click an entry handle or double-click the entry to expand or collapse a system tree entry. Click and drag the window border to re-size the window.
Action Menu	Right-click anywhere on the system tree window to open the action menu. This menu provides a shortcut to actions available elsewhere in the SANsurfer Router Manager. If you select an initiator or target (highlighted), then right-click in the system tree, the action menu activates the **Remove Initiator** and **Remove Offline Target** selections.
Information, Configuration, and Status windows	These windows present the corresponding information, configuration, or status for the window tab you select. Some windows contain a scroll bar to browse the window contents.Click and drag the window border to re-size the window.
Window Tabs	The window tab determines what is displayed in the window.

Menu Bar

Figure 2-2 shows the menu bar options. The following sections describe them.

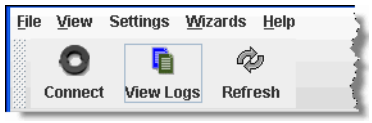

Figure 2-2 Menu Bar

File Menu

Figure 2-3 shows the **File** menu. The following paragraphs describe it.

Figure 2-3 File Menu

- **Save FRU** – Saves the router's configuration and persistent data to a file.
- **Restore FRU** – Restores the router's configuration and persistent data from a file.
- **Exit** – Exits the SANsurfer Router Manager.

View Menu

Figure 2-4 shows the **View** menu. The following paragraph describes it.

Figure 2-4 View Menu

- **View Logs** – Opens the window displaying the system logs.

Settings Menu

Figure 2-5 shows the **Settings** menu. The following paragraph describes it.

Figure 2-5 Settings Menu

- **Broadcast** – Opens the Broadcast Settings window, which allows you to configure the broadcast options. The workstation sends broadcast messages to locate routers within the same IP subnet as the workstation running the SANsurfer Router Manager application. Figure 2-6 shows the Broadcast Settings dialog box. The following paragraphs describe its options.

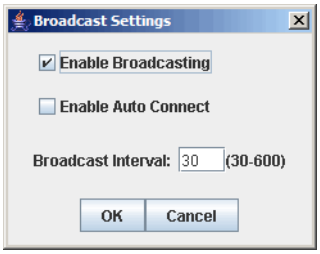

Figure 2-6 Broadcast Settings Menu

- **Enable Broadcast** – Enables broadcast messages sent to locate routers in the IP subnet.
- **Enable Auto Connect** – Enables the SANsurfer Router Manager to automatically connect with routers discovered by the broadcast.
- **Broadcast Interval** – Lets you enter the time interval at which the SANsurfer Router Manager sends broadcast messages to locate routers within the same IP subnet as the workstation.

Wizards Menu

Figure 2-7 shows the **Wizards** menu. The following paragraphs describe it.

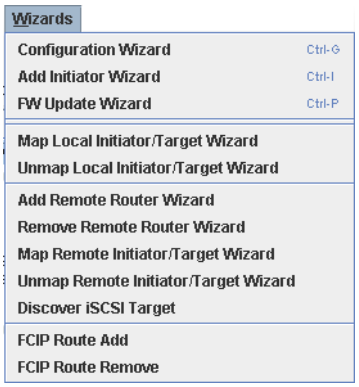

Figure 2-7 Wizards Menu

- **Configuration Wizard** – Launches the iSCSI Port Configuration Wizard, which allows you to configure the IP address and other parameters for an iSCSI port (see page 4-2).
- **Add Initiator Wizard** – Launches the iSCSI Add Initiator Wizard, which allows you to configure the IP address and other parameters for an iSCSI initiator (see page 4-7).
- **FW Update Wizard** – Launches the Firmware Update Wizard, which allows you to update the iSR6142 router's firmware image. You can select the firmware image from a menu that allows browsing (see page 4-9).

- **Map Local Initiator/Target Wizard** – Launches the Map Local Wizard, which allows you to map a local initiator to a local target (see page 4-13).
- **Unmap Local Initiator/Target Wizard** – Launches the Unmap Local Wizard, which allows you to delete a local initiator from a local target mapping (see page 4-20).
- **Add Remote Router Wizard** – Launches the Add Remote Router Wizard, which allows you to assign local router to a remote router as peers (see page 4-25).
- **Remove Remote Router Wizard** – Launches the Remove Remote Router Wizard, which allows you to remove a local-to-remote router peer assignment (see page 4-30).
- **Map Remote Initiator/Target Wizard** – Launches the Map Remote Wizard, which allows you to map an initiator to a target device, one of which is on a remoter router (see page 4-33).
- **Unmap Remote Initiator/Target Wizard** – Launches the Unmap Remote Wizard, which allows you to delete an initiator-to-target device mapping (see page 4-20).
- **Discover iSCSI Target** – Launches the Discover iSCSI Target Wizard, which allows you to specify the IP address of the iSCSI Target to be discovered. The target is added to the discovered targets list (see section page 4-42).
- **FCIP Route Add** – Launches the (Fibre Channel over IP) FCIP Route Add Wizard, which allows you to select the resources used for the route, the IP address of the remote FCIP peer, IP parameters, Virtual Lan (VLAN) support, compression, and bandwidth limit (see page 4-45).
- **FCIP Route Remove** – Launches the FCIP Route Remove Wizard, which allows you to remove an existing FCIP route, freeing the resources (FC and GE ports) used by the route (see page 4-51).

Help Menu

Figure 2-8 shows the **Help** menu. The following paragraphs describe it.

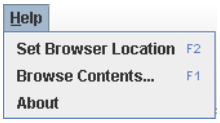

Figure 2-8 Help Menu

Set Browser Location – Allows you to specify the browser that launches when you view the online help for the SANsurfer Router Manager.

Browse Contents – Launches the online help for the SANsurfer Router Manager.

About – Displays the application version information.

Tool Bar

Figure 2-9 shows the tool bar. The following paragraphs describe it.

Figure 2-9 Tool Bar

The tool bar consists of a row of graphical buttons that allow you to perform common functions: connect, view log files, and refresh the current display. You can move the tool bar in the display by clicking and dragging the handle at the tool bar's left edge.

- **Connect** – Adds an iSR6142 router to the system tree view.
- **View Logs** – Opens a window to display the system log data.
- **Refresh** – Updates the display with current information.

Action Menu

The action menu provides short cuts to actions and wizards available elsewhere in the SANsurfer Router Manager. To open this menu, right-click anywhere within the router's node in the system tree window. Figure 2-10 illustrates the action menu and the following paragraphs describe each available option.

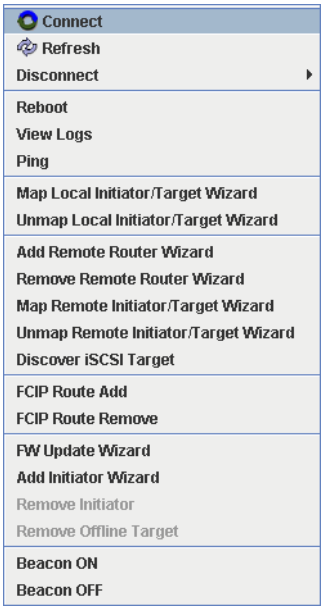

Figure 2-10 Action Menu

- **Connect** – Adds an iSR6142 router to the system tree view.
- **Refresh** – Updates the display with current information.
- **Disconnect** – Disconnects from an iSR6142 router, removing it from the system tree.
- **Reboot** – Reboots the iSR6142 router.
- **View Logs** – Opens the View Logs window.
- **Ping** – Initiates a ping from the specified port (management, GE1, or GE2) to a specified IP address.
- **Map Local Initiator/Target Wizard** – Launches the Map Local Initiator/Target Wizard, which allows you to map a local initiator to a local target (see page 4-13).
- **Unmap Local Initiator/Target Wizard** – Launches the Unmap Local Initiator/Target Wizard, which allows you to delete a local initiator from a local target mapping (see page 4-20.)

- **Add Remote Router Wizard** – Launches the Add Remote Router Wizard, which allows you to assign local router to a remote router as peers (see page 4-25).
- **Remove Remote Router Wizard** – Launches the Remove Remote Router Wizard, which allows you to remove a local-to-remote router peer assignment (see page 4-30).
- **Map Remote Initiator/Target Wizard** – Launches the Map Remote Initiator/Target Wizard, which allows you to map an initiator to a target device, one of which is on a remoter router (see page 4-33).
- **Unmap Remote Initiator/Target Wizard** – Launches the Unmap Local Initiator/Target Wizard, which allows you to delete an initiator-to-target device mapping (see page 4-20).
- **Discover iSCSI Target** – Launches the Discover iSCSI Target Wizard, which allows you to specify the IP address of the iSCSI target to be discovered. The target is added to the discovered targets list (see page 4-42).
- **FCIP Route Add** – Launches the FCIP Route Add Wizard, which allows you to select the resources used for the route, the IP address of the remote FCIP peer, IP parameters, VLAN support, compression, and bandwidth limit (see page 4-45).
- **FCIP Route Remove** – Launches the FCIP Route Remove Wizard, which allows you to remove an existing FCIP route, freeing the resources (FC and GE ports) used by the route. (See page 4-51).
- **FW Update Wizard** – Launches the FW Update Wizard, which allows you to update the router's firmware (see page 4-9).
- **Add Initiator Wizard** – Launches the Add Initiator Wizard, which allows you to enter an iSCSI initiator into the system database (see page 4-7).
- **Remove Initiator** – Removes the selected iSCSI initiator. This option is available only when an initiator is selected (highlighted) in the system tree.
- **Remove Offline Target** – Removes the selected offline Fibre Channel target. This option is available only when an offline FC target is selected (highlighted) in the system tree.
- **Beacon ON** – Turns on the **iSR6142** router beacon to locate the router quickly.
- **Beacon OFF** – Turns off the **iSR6142** router beacon.

System Tree Window

Figure 2-11 shows the system tree window. The following sections described it.

Figure 2-11 System Tree Window

The left-most window pane shows the system tree. The system tree includes the connected iSR6142 routers and the following components for each router:

- FC Ports (see page 3-11)
- iSCSI Ports (see page 3-14)
- Discovered iSCSI Initiators (see page 3-22)
- FC Discovered Targets (see page 3-25)
- iSCSI Discovered Targets (see page 3-29)
- FCIP Routes (see page 3-30)

Select a component in the system tree to see component data in the tabbed pages to the right of the tree (see page 2-11).

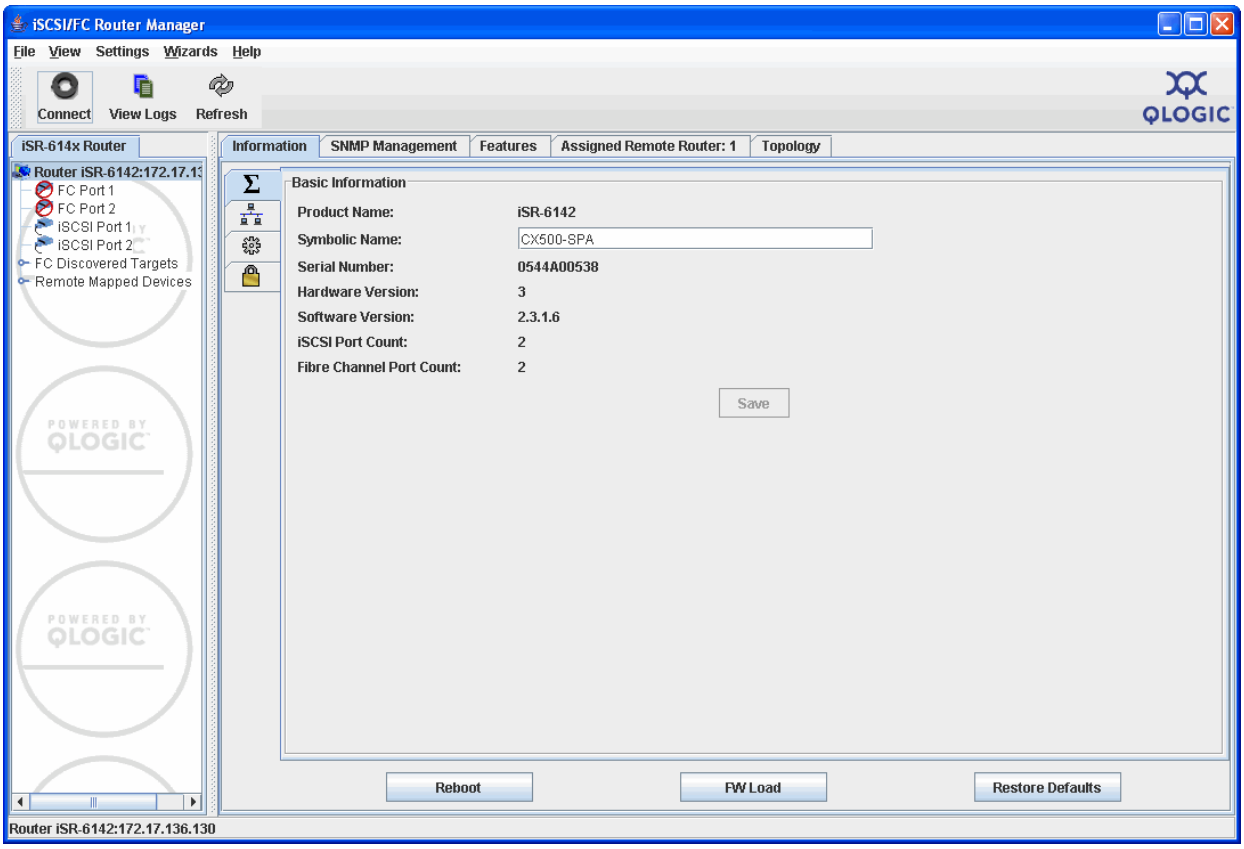

Figure 2-12 Component Information

Component information displayed for a selected router includes router information, configuration details, router status, and lists of connected or discovered devices.

Notes

3 Managing the Router

The SANsurfer Router Manager lets you monitor and manage the iSR6142 router, as well as its ports and connected devices by viewing and selecting components in the system tree. The following sections describe these components:

- "iSR6142 Router" on page 3-1
- "FC Ports" on page 3-11
- "iSCSI Ports" on page 3-14
- "Discovered iSCSI Initiators" on page 3-22
- "FC Discovered Targets" on page 3-25
- "iSCSI Discovered Targets" on page 3-29
- "FCIP Routes" on page 3-30

iSR6142 Router

The top of the router tree displays the router system configuration and status. It contains the following tabs:

- Information Tab (see page 3-2)
- SNMP Management Tab (see page 3-7)
- Features Tab (see page 3-9)
- Assigned Remote Router Tab (see page 3-9)
- Topology Tab (see page 3-10)

NOTE:

If your router's configuration includes a remote router, the router configuration window includes a tab with the basic information for that router, as shown in the following example for **Assigned Remote Router:1**. You can define additional remote routers using the Add Remote Router Wizard.

Information Tab

The Information tab provides four vertical tabs with icons that identify its content: Basic Information, Management Information, and NTP Server Information, and Security. It also contains three buttons: **Reboot**, **FW Load**, and **Restore Defaults**.

Basic Information

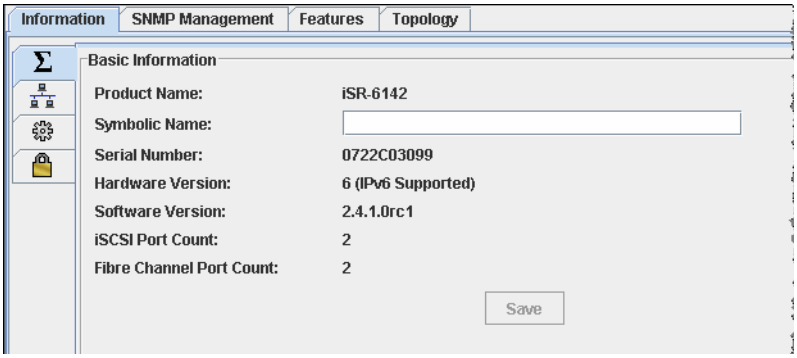

Figure 3-1 Basic Information Vertical Tab

The Basic Information tab provides the following parameters:

- **Product Name** – Identifies the router model.
- **Symbolic Name** – Lets you to assign a symbolic name to the router.
- **Serial Number** – Displays the router's serial number.
- **Hardware Version** – Identifies the router hardware version number.
- **Software Version** – Identifies the version of firmware loaded on the router.
- **iSCSI Port Count** – Identifies the number of iSCSI ports (2).
- **Fibre Channel Port Count** – Identifies the number of Fibre Channel ports (2).

Management Information

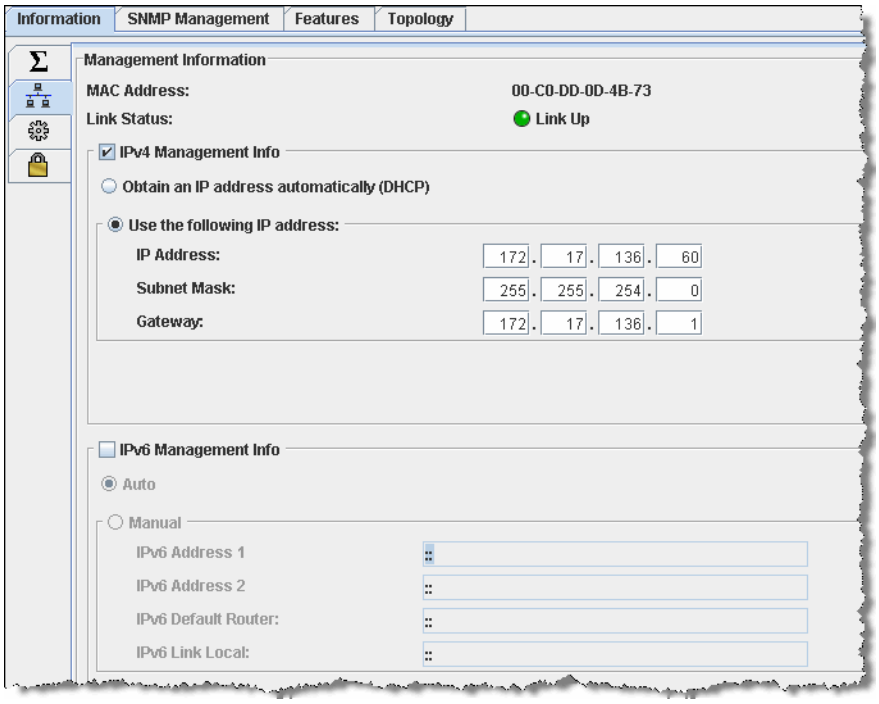

Figure 3-2 Management Information Vertical Tab

The Management Information tab provides the following parameters:

- **MAC Address** – Displays the management port's MAC address.
- **Link Status** – Displays the management port link status: **Link Up** or **Link Down**.

- **IPv4 Management Info** – Select this check box to use IPv4 (Internet Protocol version 4, 32-bit addressing), then use the radio buttons to identify whether to use a dynamic or static IP address.
  - **IP Address** – Displays the management port's subnet mask.
    - If you selected the **Obtain an IP address automatically (DHCP)** radio button, the system obtains the IP address automatically through DHCP.
    - If you selected the **Use the following IP address** radio button, you can configure the IP address.
  - **Subnet Mask** – Displays the management port's subnet mask.
    - If you select the **Obtain an IP address automatically (DHCP)**, the system obtains the subnet mask automatically through DHCP.
    - If you selected the **Use the following IP address** radio button, you can configure the subnet mask.
  - **Gateway** – Displays the IP address of the server acting as a gateway to your Internet connection.
    - If you select the **Obtain an IP address automatically (DHCP)**, the system obtains the gateway address automatically through DHCP.
    - If you selected the **Use the following IP address** radio button, you can specify the gateway address.
- **IPv6 Management Info** – Select this check box to use IPv6 (Internet Protocol version 6, 128-bit addressing), then use the radio buttons to identify whether to use a dynamic or static IP address.
  - **IPv6 Management Info –** Select this check box if you want to use IPv6, then use the radio buttons to identify whether to use a dynamic or static IP address.
  - **IPv6 Address1** – The first user-assigned IPv6 address to which the port responds. A value of :: indicates that an IPv6 address has not been assigned. Although you may modify the IP address in this window, you will typically set it using the Configuration Wizard.
  - **IPv6 Address2** – The second user-assigned IPv6 address to which the port responds. A value of :: indicates that an IPv6 address has not been assigned. Although you may modify the IP address in this window, you will typically set it using the Configuration Wizard.

- **IPv6 Default Router** – Use this address to set the default router for the IPv6. The system can also set the IPv6 default router dynamically depending on your network configuration.
- **IPv6 Local Link** – This field contains the IPv6 link local address of the port. It is not editable.

NOTE:

IPv6 support is available only with hardware version 6 and software version 2.4.0.0 and greater.

- **Set IP Address** – After making any IP address changes, click this button to save your changes.

NTP Server Information

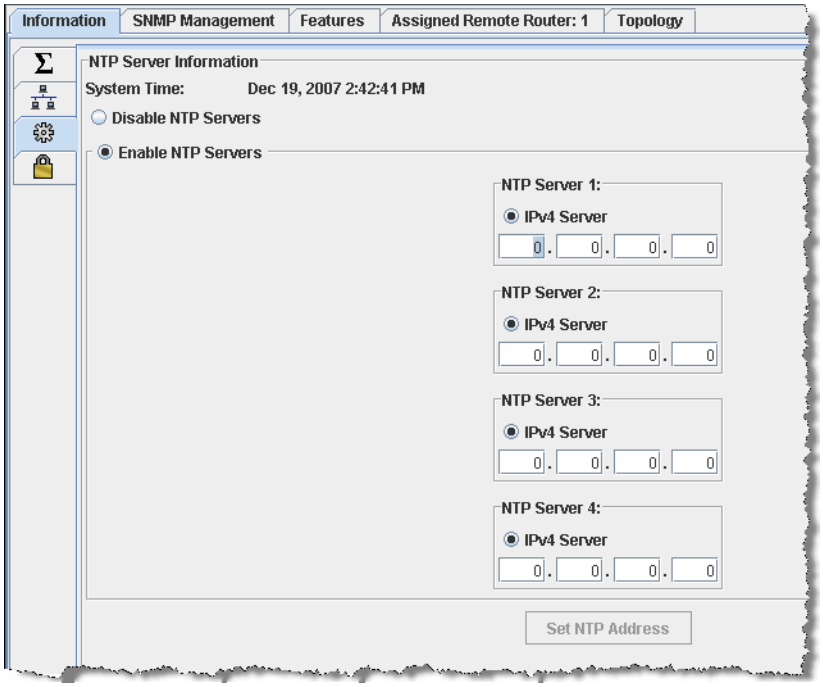

Figure 3-3 NTP Server Information Vertical Tab

The NTP Server Information tab provides the following parameters:

- **NTP Server Radio Buttons** – Use these buttons to disable or enable using NTP servers to set the router's date and time.
- **NTP Server 1** – Displays the IP address of the first NTP server to be queried by the router when setting its time and date.

- **NTP Server 2** – Displays the IP address of the second NTP server to be queried by the router when setting its time and date. This server is used only if the first NTP server did not respond.
- **NTP Server 3** – Displays the IP address of the third NTP server to be queried by the router when setting its time and date. This server is used only if the first and second NTP servers did not respond.
- **NTP Server 4** – Displays the IP address of the fourth NTP server to be queried by the router when setting its time and date. This server is used only if the first, second, and third NTP servers did not respond.
- **Set NTP Address** – After enabling NTP servers and setting their IP addresses, click this button saves any changes made to the NTP server IP addresses.

Security

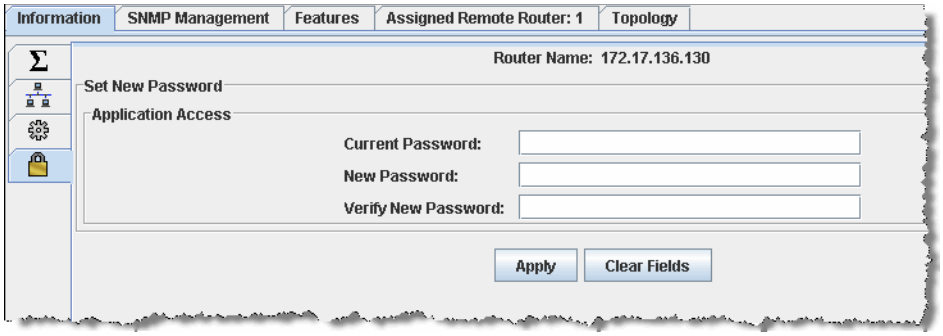

Figure 3-4 Security Vertical Tab

The Security tab enables you to set the router's password. The Security tab provides the following parameters:

- **Current Password** – You must enter the current password before changing it.
- **New Password** – Enter the new router password.
- **Verify New Password** – Verify the password entered in the **New Password** field.
- **Apply** – Click this button to save the password changes.
- **Clear Fields** – Click this button to clear the **Current Password**, **New Password**, and **Verify Password** fields.

SNMP Management Tab

The SNMP Management tabbed page consists of two sections: SNMP Configuration and SNMP Trap Receivers. The **Save** button saves any SNMP management changes. For more information, see Appendix B.

Figure 3-5 shows the SNMP Management tabbed page. The following paragraphs describe it.

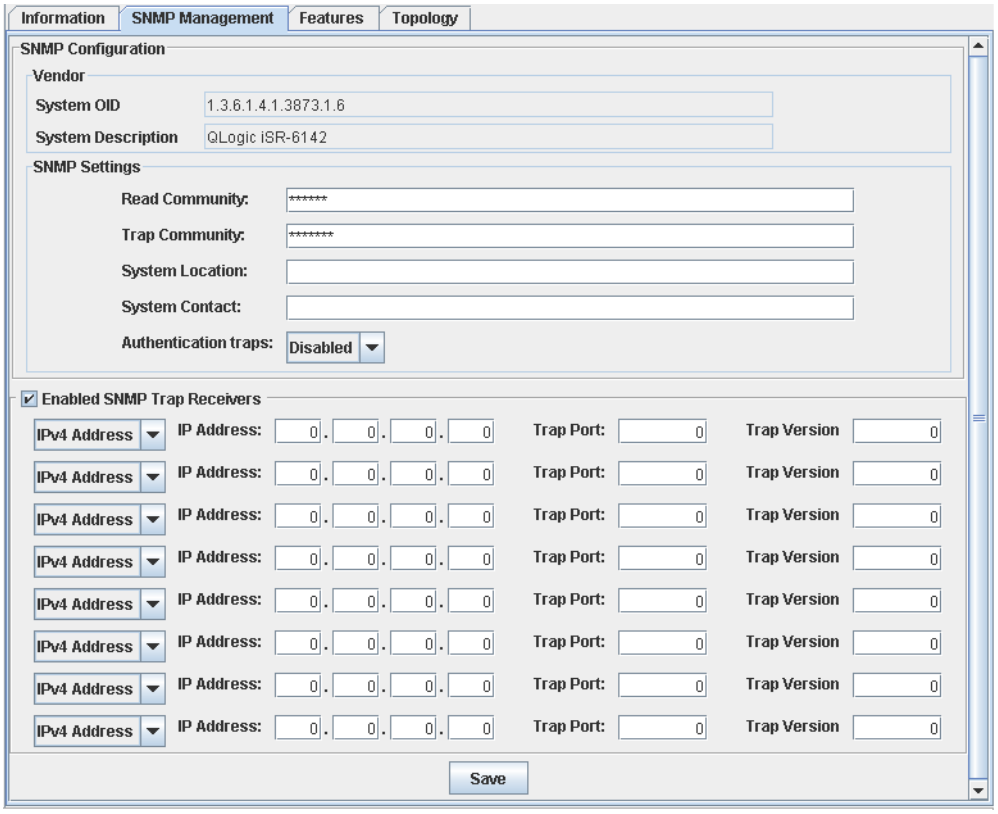

Figure 3-5 SNMP Management Tabbed Page

The SNMP Management tab provides two configuration sections:

- SNMP Configuration
- SNMP Trap Receivers

SNMP Configuration

The SNMP Configuration section provides the following vendor and SNMP setting fields:

- **System OID** – Displays the system object identifier.
- **System Description** – Displays a description of the router location.

- **Read Community** – Enter a password that authorizes an SNMP management server to read information from the router. This is a write-only field. The value on the router and the SNMP management server must be the same. The read community password can be up to 32 characters excluding #, semicolon (;), and comma (,). The default is public.
- **Trap Community** – Enter a password that authorizes an SNMP management server to receive traps. This is a write-only field. The value on the router and the SNMP management server must be the same. The trap community password can be up to 32 characters excluding the number sign (#), semicolon (;), and comma (,). The default is public.
- **System Location** – Specifies the name of the router location. The name can be up to 64 characters excluding the number sign (#), semicolon (;), and comma (,).
- **System Contact** – Specifies the name of the person to be contacted to respond to trap events. The name can be up to 64 characters excluding the number sign (#), semicolon (;), and comma (,).
- **Authentication Traps** – Enables or disables the generation of authentication traps in response to authentication failures.

SNMP Trap Receivers

- **Enabled** – Select this check box next to each trap receiver you want to configure, then use the following fields to specify its IP address, trap port, and trap version.
- **IP Protocol** – Select the IP protocol version from the drop-down menu: IPv6 Address or IPv4 Address. The IP address field changes to accept the appropriate format.
- **IP Address** – Specifies the IP address to which the SNMP traps are sent. A maximum of eight trap addresses are supported.
- **Trap Port** – Identifies the port number on which the trap is sent. The default is 162.
- **Trap Version** – Specifies the SNMP version (1 or 2) with which to format traps.

Features Tab

Figure 3-6 shows the Features tabbed page that displays the router's licensed features and lets you apply additional license features. The following paragraphs described the page.

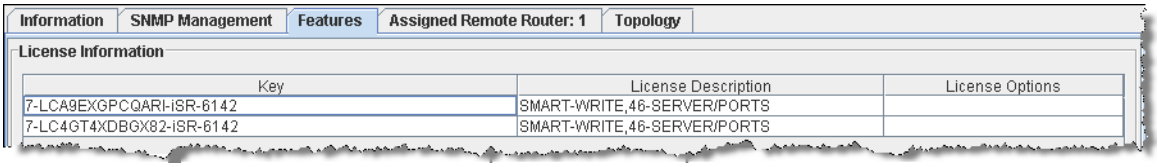

Figure 3-6 Features Tabbed Page

- **License Information** – Displays a list of the router's licensed features.
- **Add** – Initiates the Add Feature Wizard.

Assigned Remote Router Tab

If your local router has any remote routers added as peers to its configuration, the iSR6142 router screen includes a tabbed page for each assigned remote router.

This screen provides the following information about the remote router:

- **Product Name** – Identifies the model of the remote router.
- **Symbolic Name** – Displays the symbolic name, if one is assigned to the remote router.
- **Serial Number** – Displays the remote router's serial number.
- **Hardware Version** – Identifies the remote router hardware version number. Starting with version 6, the hardware supports IPv6.
- **Software Version** – Identifies the version of firmware loaded on the remote router. IPv6 requires software version 2.4.0.0 or later.
- **iSCSI Port Count** – Identifies the number of iSCSI ports (2).
- **Management IP Address** – Displays the IP address of the remote router.

Topology Tab

Figure 3-7 shows the Topology tabbed page that displays the routers, as shown in the following example.

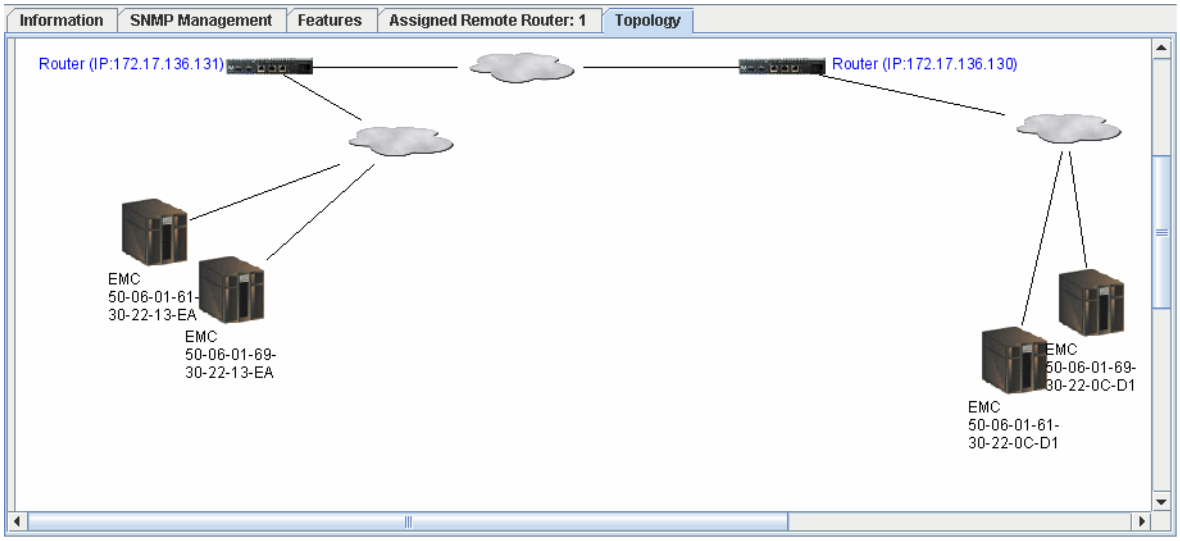

Figure 3-7 Topology Tabbed Page

FC Ports

When you select an FC port in the system tree, the system displays the FC Port Information tabbed page (see Figure 3-8).

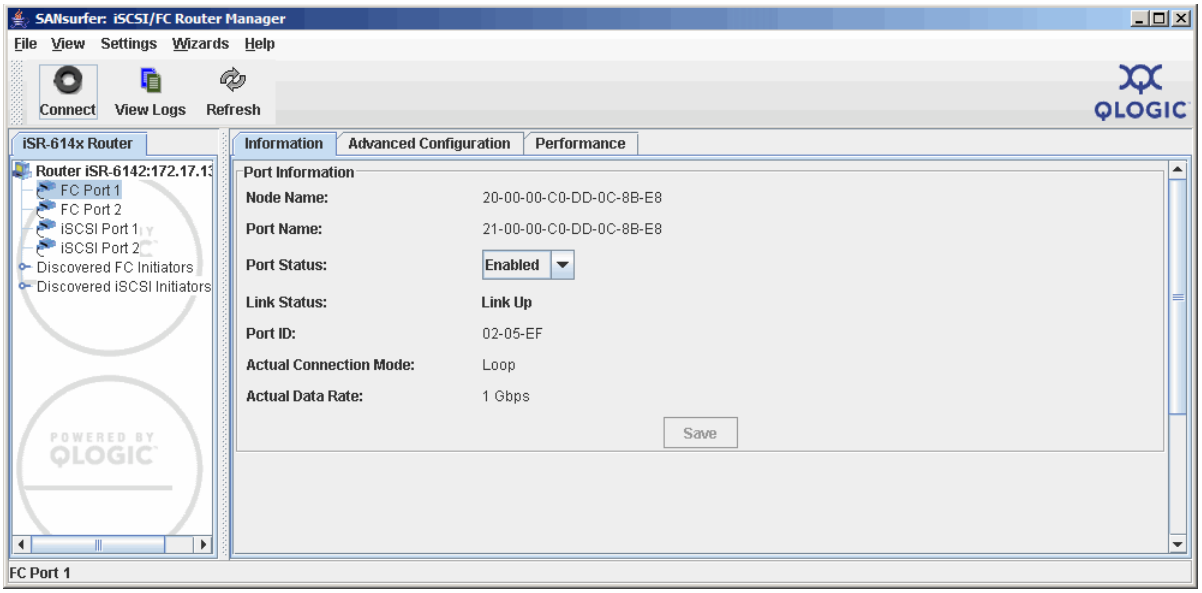

Figure 3-8 FC Port Information Tab

FC Port Information Tab

The FC Port Information tab provides the following parameters:

- **Node Name** – Displays the world-wide node name (WWNN) assigned to the FC port.
- **Port Name** – Displays the world-wide port name (WWPN) assigned to the FC port.
- **Port Status** – Lets you change the port status: **Enabled** (online) or **Disabled** (offline). After changing the status, click **Save**. If you choose to disable the port, a warning message appears, letting you know it will disconnect one or more ports. Click **Yes** to disconnect the port, or **No** to cancel the changes.
- **Link Status** – Displays the link status, either `Link Up` or `Link Down`.
- **Port ID** – Displays the ID assigned by the FC fabric or `AL_PA` if the FC port is connected to a private loop.

- **Actual Connection Mode** – Displays the port's connection mode, either `Point-to-Point` or `Loop`.
- **Actual Data Rate** – Displays the port's operating data rate when online, either one gigabit per second (`1 Gbps`) or two gigabits per second (`2 Gbps`).

FC Port Advanced Configuration Tab

When you select the **Advanced Configuration** tab for the selected FC port, the system displays the Advanced Configuration tabbed page (see Figure 3-9).

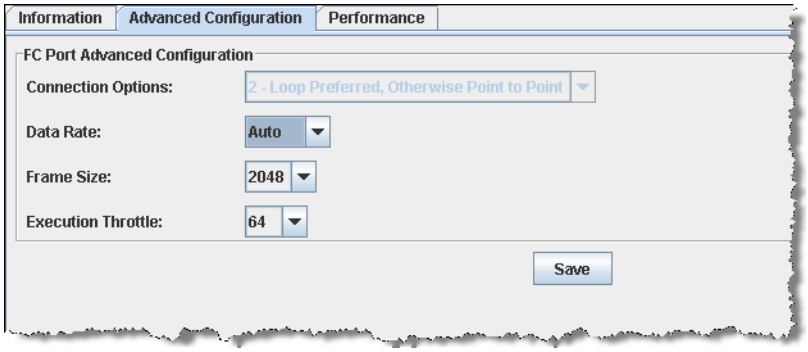

Figure 3-9 FC Port Advanced Configuration Tab

The FC port Advanced Configuration tab provides the following parameters:

- **Connection Options** – Displays the connections. When an FC port is not part of an FCIP route, it only operates in FC loop mode.
- **Data Rate** – Displays a drop-down list that lets you set the data rate: **Auto**, **1 Gbps**, or **2 Gbps**. The default is **Auto**. If you change this setting, you must click **Save** (at the bottom of the page) for the change to take effect.
- **Frame Size** – Displays a drop-down list that lets you set the frame size: **2048**, **1024**, or **512** bytes. The default is **2048**. If you change this setting, you must click **Save** (at the bottom of the page) for the change to take effect.
- **Execution Throttle** – Displays a drop-down list that lets you set the execution throttle: **16**, **32**, **64**, **128**, or **256**. The default is **64**. When you change this setting, you must click **Save** (at the bottom of the page) for the change to take effect.

FC Port Performance Tab

When you select the **Performance** tab for the selected FC port, the system displays the Performance tabbed page (see Figure 3-10).

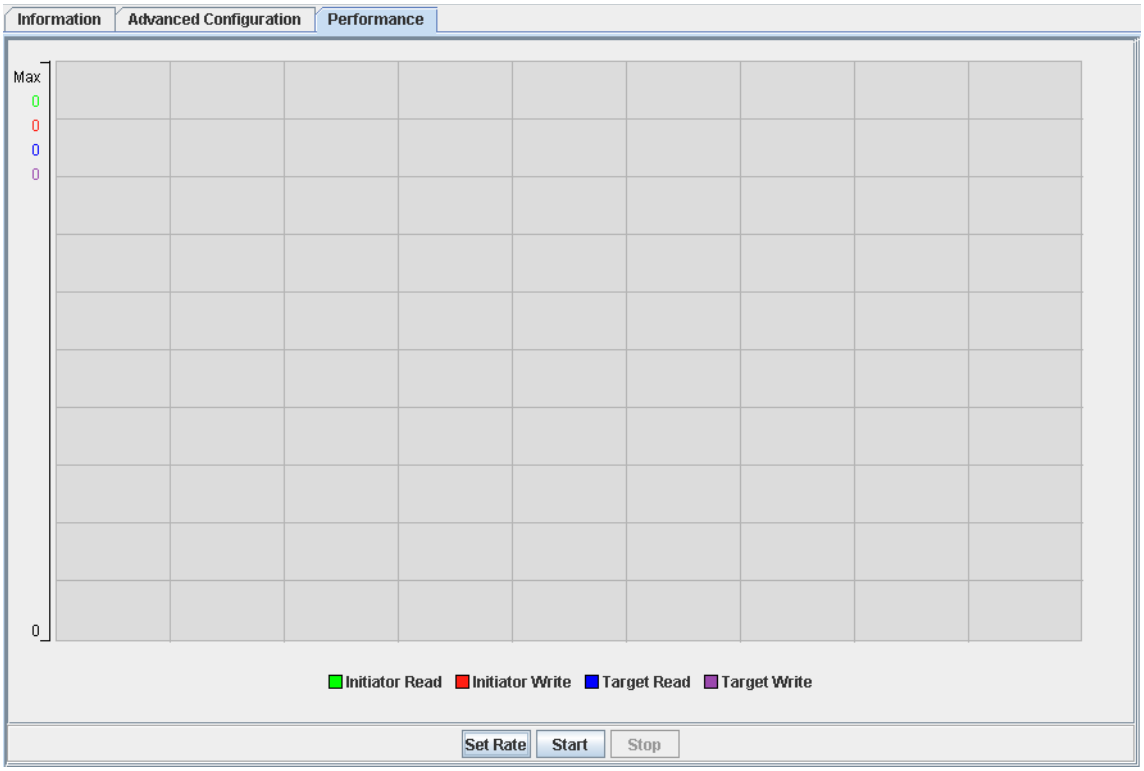

Figure 3-10 FC Port Performance Tab

The FC Port Performance tab displays the following information:

- **Initiator Read** – Shows the initiator's read performance through the selected FC port.
- **Initiator Write** – Shows the initiator's write performance through the selected FC port.
- **Target Read** – Shows the target's read performance through the selected FC port.
- **Target Write** – Shows the target's write performance through the selected FC port.

iSCSI Ports

When you select an iSCSI port in the system tree, the window displays the Information, Advanced Configuration, and Statistics tabbed pages to the right of the tree (see Figure 3-11). These following sections describe these pages.

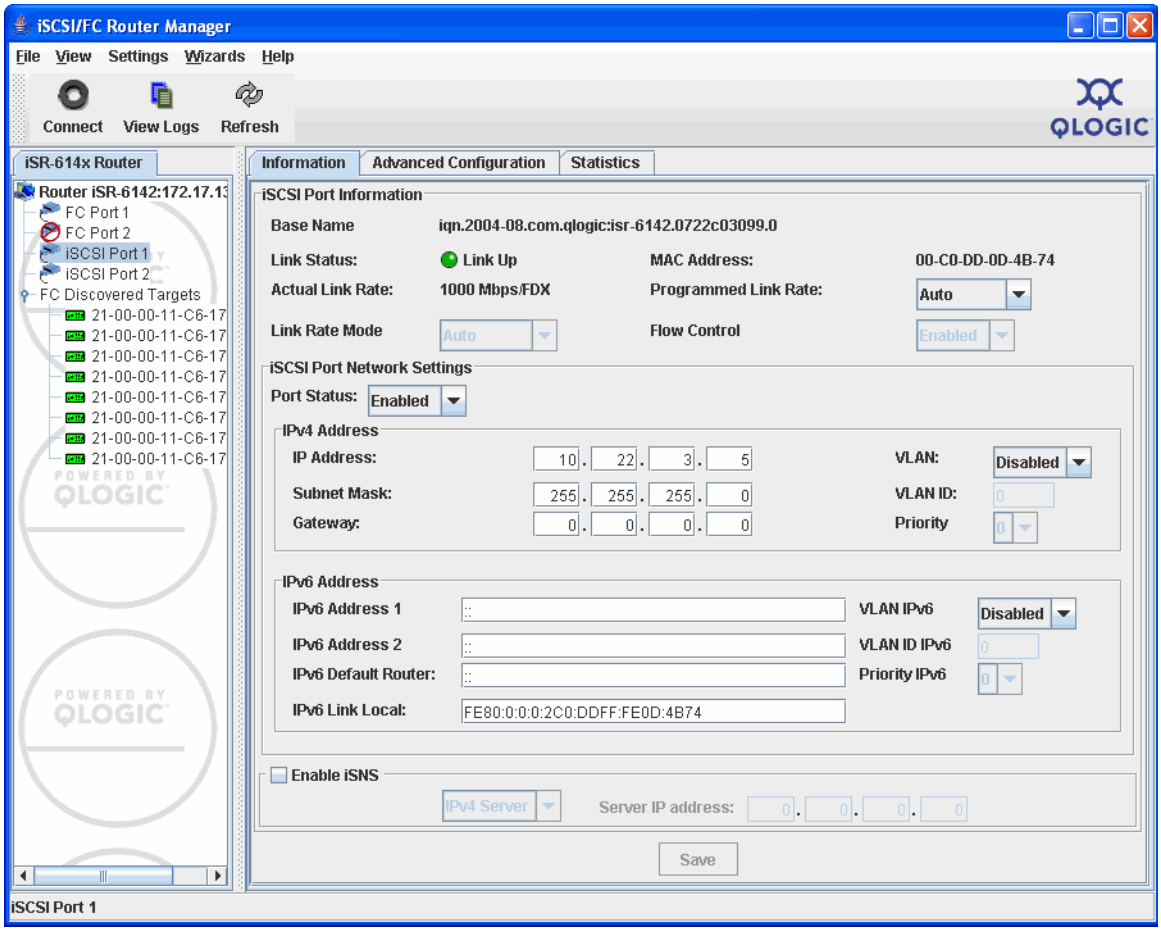

Figure 3-11 iSCSI Port Tabbed Pages

Information Tab

The Information tabbed page consists of three areas: Port Information, iSCSI Port Network Settings, and iSNS. The following paragraphs describe the information displayed in these sections.

iSCSI Port Information

The iSCSI Port Information area provides the following parameters:

- **Base Name** – Displays the full name assigned to the selected iSCSI port.
- **Link Status** – Identifies the port connection status: `Link Up` or `Link Down`.
- **MAC Address** – Displays the MAC address assigned to the port. The MAC address is not changeable.
- **Actual Link Rate** – Displays the actual link rate, which can be `Unknown`, `1000 Mbps`, `100 Mbps`, or `10 Mbps`. If the port's configuration or connection has changed, the status may not be current. Click the **Refresh** icon to display the current status.
- **Programmed Link Rate** – The configured data rate for the port. To configure the data rate, open the drop-down menu and select one of the following data rates:
  - **Auto** - Data rate determined by network attachment
  - **10 Mbps** - 10 megabits per second
  - **100 Mbps** - 100 megabits per second
  - **1000 Mbps** - 1000 megabits per second (1 gigabit per second)

  When you change this setting, you must click **Save** (at the bottom of the page) for the change to take effect.
- **Link Rate Mode** – If you selected a specific **Programmed Link Rate** (not **Auto**), you can specify one of these modes:
  - **Auto**
  - **Half Duplex**
  - **Full Duplex**
- **Flow Control** – If you selected a specific **Programmed Link Rate** (not **Auto**), you can enable or disable flow control.

iSCSI Port Network Settings

- **Port Status** – When the port link is up, you can enable or disable the port using this drop-down list.
- **IPv4 Address** – When using an IPv4 address scheme, define the following fields:
  - **IP Address** – The IP address to which the port responds. An un-initialized port has an IP address of all zeros. Although you may modify the IP address in this window, you will typically set it using the Configuration Wizard.
  - **Subnet Mask** – The subnet mask used by the port. Although you may modify the subnet mask in this window, you will typically set it using the Configuration Wizard.
  - **Gateway** – The gateway for the selected port.
  - **VLAN** – The VLAN configuration: **Disabled** or **Enabled**. You can configure VLAN from this window.
  - **VLAN ID** – When VLAN is enabled the **VLAN ID** contains an identification value in the range `0` to `4094`. You can configure VLAN from this window.
  - **Priority** – When VLAN is enabled, this field defines the priority assigned to this VLAN. To set the priority, open the drop-down menu and select the desired value (between **0** to **7**).
- **IPv6 Address** – When using an IPv6 address scheme, define the following fields:
  - **IPv6 Address1** – The first user-assigned IPv6 address to which the port responds. A value of :: indicates that an IPv6 address has not been assigned. Although you may modify the IP address in this window, you will typically set it using the Configuration Wizard.
  - **IPv6 Address2** – The second user-assigned IPv6 address to which the port responds. A value of :: indicates that an IPv6 address has not been assigned. Although you may modify the IP address in this window, you will typically set it using the Configuration Wizard.
  - **IPv6 Default Router** – Use this address to set the default router for the IPv6. The system can also set the IPv6 default router dynamically depending on your network configuration.
  - **IPv6 Local Link** – This field contains the IPv6 link local address of the port. It is not editable.
  - **VLAN IPv6** – The VLAN IPv6 configuration: **Disabled** or **Enabled**. You can configure VLAN from this window.

- **VLAN ID IPv6** – When VLAN IPv6 is enabled the VLAN ID IPv6 contains an identification value in the range `0` to `4094`. You can configure VLAN from this window.
- **Priority IPv6** – When VLAN IPv6 is enabled, this field defines the priority assigned to this VLAN IPv6. To set the priority, open the drop-down menu and select the desired value (between **0** to **7**).

NOTE:

IPv6 support is available only with hardware version 6 and greater and software version 2.4.0.0 and greater.

- **Enable iSNS** – This check box enables or disables iSNS support. Select the check box to enable this option; clear the check box to disable it.
  - **IP Server –** This drop-down box lets you choose the IP address version assigned to the IP server. The following examples show the IP address fields that open when you choose one of these options.
  - **Server IP Address** – The IP address assigned to the iSNS server to which this port will communicate. You can configure this IP address when iSNS is enabled. Note the different formats provided for the two different IP address version.

Advanced Configuration Tab

The Advanced Configuration tabbed page allows you to configure the router's port parameters, security settings, and CHAP settings. The information displayed in these sections is illustrated in Figure 3-12 and described in the following paragraphs.

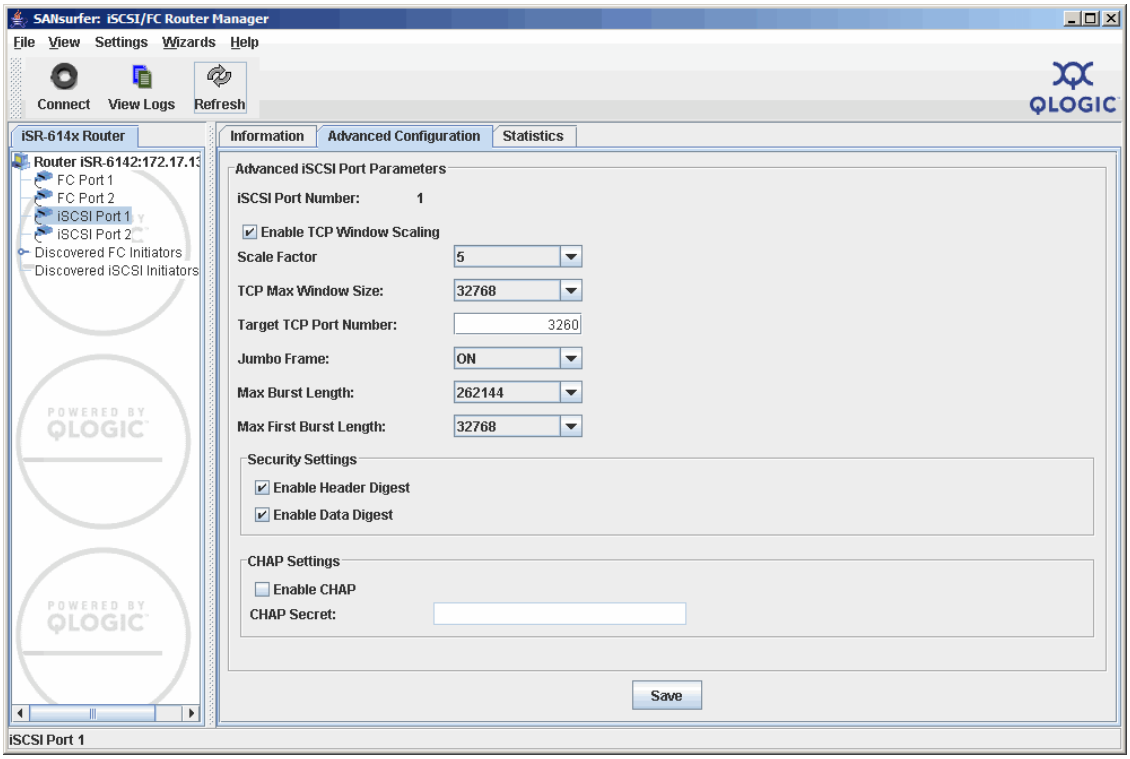

Figure 3-12 Advanced Configuration Tabbed Page

The iSCSI Port Advanced Configuration tab provides the following parameters:

- **iSCSI Port Number** – Identifies the iSCSI port number (1 or 2).
- **Enable TCP Window Scaling** – When you change this setting, you must enter the **Scale Factor** (valid values are 0–5), then click **Save** (at the bottom of the page) for the change to take effect.
- **TCP Max Window Size** – Enables you to set the TCP maximum window size. To change the setting, open the drop-down menu and select one of the options: **8192**, **16384**, or **32768**.

- **Target TCP Port Number** – Identifies the TCP port number the router uses to receive iSCSI target commands. The iSCSI community uses TCP port number `3260` by default any change to this TCP port number requires a corresponding change in all iSCSI initiators connecting to this iSCSI target port. When you change the target TCP port number, you must click **Save** (at the bottom of the page) for the change to take effect.
- **Jumbo Frame** – Enables or disables router jumbo frame size as the maximum transfer unit (MTU). Disabling this option sets the port to support `1500` byte MTU. Enabling this option sets the port to support `9000` bytes MTU. To change this setting, select **Enabled** or **Disabled** from the drop-down menu. When you change this setting, you must click **Save** (at the bottom of the page) for the change to take effect.

  NOTE:

  An MTU size greater than 1500 should only be used when the router is connected to a 1000 Mbps Ethernet network.

- **Max Burst Length** – Enables you to set the iSCSI maximum burst length. To change this setting, select the desired value (ranging from **512** to **262144** bytes) from the drop-down menu.
- **Max First Burst Length** – Enables you to set the iSCSI maximum first burst length. To change this setting, select the desired value (ranging from **512** to **262144** bytes) from the drop-down menu.
- **Security Settings**
  - **Enable Header Digest** – Enables or disables support for iSCSI header digest. Header digest is an ISCSI feature that adds a validity check field to iSCSI PDU headers to verify that no corruption has occurred during the transmission of the PDU header. The iSR6142 router supports digest in its hardware to maximize performance. When you change this setting, you must click **Save** (at the bottom of the page) for the change to take effect.
  - **Enable Data Digest** – Enables or disables support for iSCSI data digest. Data digest is an ISCSI feature that adds a validity check to iSCSI data to verify that no corruption has occurred during the transmission of the data. The iSR6142 router supports data digest in its hardware to maximize performance. When you change this setting, you must click **Save** (at the bottom of the page) for the change to take effect.

- **CHAP Settings**
  - **Enable CHAP** – Enables or disables CHAP (Challenge Handshake Authentication Protocol) support. Select the check box to enable this option; clear the check box to disable it. When you change this setting, you must click **Save** (at the bottom of the page) for the change to take effect.
  - **CHAP Secret** – Lets you define the CHAP secret used for authenticating an iSCSI client. The field is available only when the **Enable CHAP** check box is checked. When you change the **CHAP Secret** setting, you must click **Save** (at the bottom of the page) for the change to take effect.

Statistics Tab

The Statistics tabbed page consists of a scrollable table of parameters and values. The table is divided into two sections: the first section contains statistics that are port specific, and the second section contains shared statistics (common to both iSCSI ports).

You can refresh the statistics are by clicking **Refresh** at the top of the scrollable window. You can clear the statistics (set all values to zero) by clicking **Clear**.

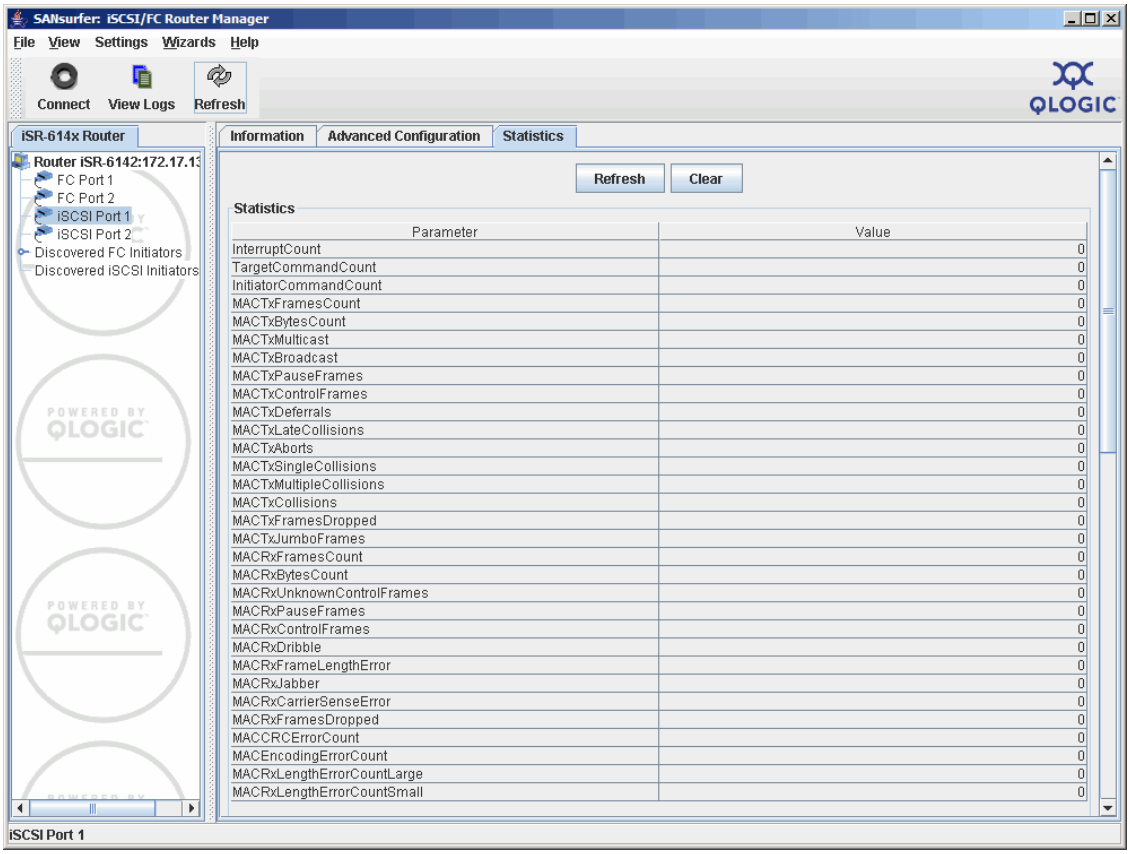

Figure 3-13 iSCSI Statistics Tabbed Page

Discovered iSCSI Initiators

Selecting the Discovered iSCSI Initiators branch on the system tree does not provide any information in the right window. Select a discovered iSCSI initiator in the system tree to display the Information and LUN List tabbed pages to the right of the system tree, which are shown in Figure 3-14 and described in the following sections.

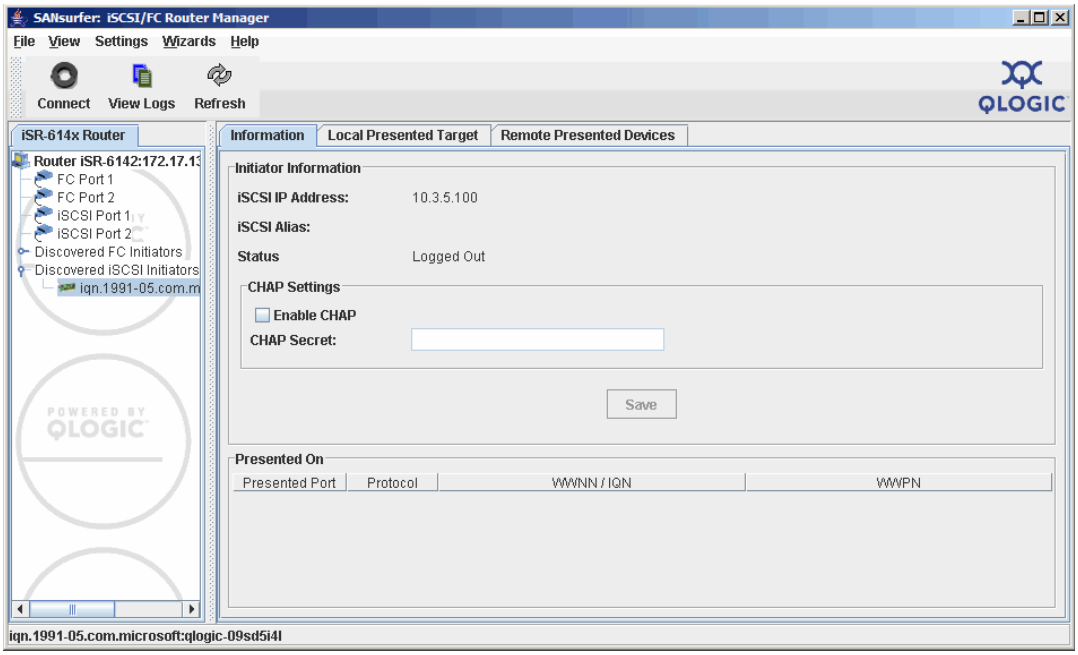

Figure 3-14 Discovered iSCSI Initiator Tabbed Pages

Information Tab

The Information tabbed page consists of two sections: Initiator Information and CHAP Settings. The following paragraphs describe the information displayed in these sections.

The **Initiator Information** section provides the following parameters:

- **iSCSI IP Address** – Displays the IP address of the discovered iSCSI initiator.
- **iSCSI Alias** – Displays the iSCSI initiators alias, which the initiator provides when it logs into the iSR-6142 router.
- **Status** – Displays the activity status for the selected initiator.

The CHAP Settings section provides the following parameters:

- **Enable CHAP** – Enables or disables CHAP (Challenge Handshake Authentication Protocol) support. Select the check box to enable this option; clear the check box to disable it.
- **CHAP Secret** – Lets you define the CHAP secret used for authenticating an iSCSI client. The field is available only when the CHAP check box is checked.

NOTE:

To apply any changes, click the **Save** button, located at the bottom of window.

Local Presented Target Tab

The Local Presented Target tabbed page consists of a scrollable list of logical unit numbers (LUNs) mapped to the iSCSI initiator, as shown in Figure 3-15 and described in the following paragraphs.

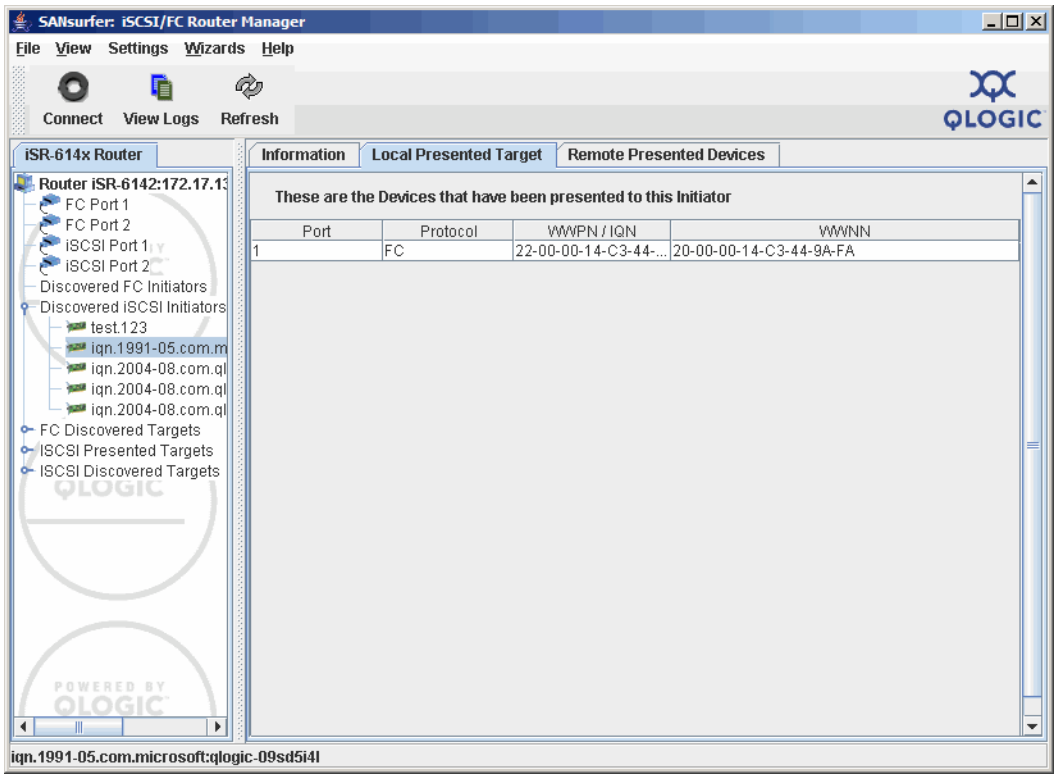

Figure 3-15 Local Presented Target Tabbed Page

- **Port** – Displays information provided by the target LUN as a result of issuing a SCSI Inquiry command.
- **Protocol** – Identifies the target name. For FC targets, the name is the WWPN.
- **WWPN/IQN** – Specifies the world-wide unique LUN name (WWULN), also provided on page 83 of a SCSI Inquiry command.
- **WWNN** – Shows the logical unit number.

Remote Presented Target Tab

The Remote Presented Target tabbed page consists of a scrollable list of LUNs mapped to the iSCSI initiator, as shown in Figure 3-16 and described in the following paragraphs.

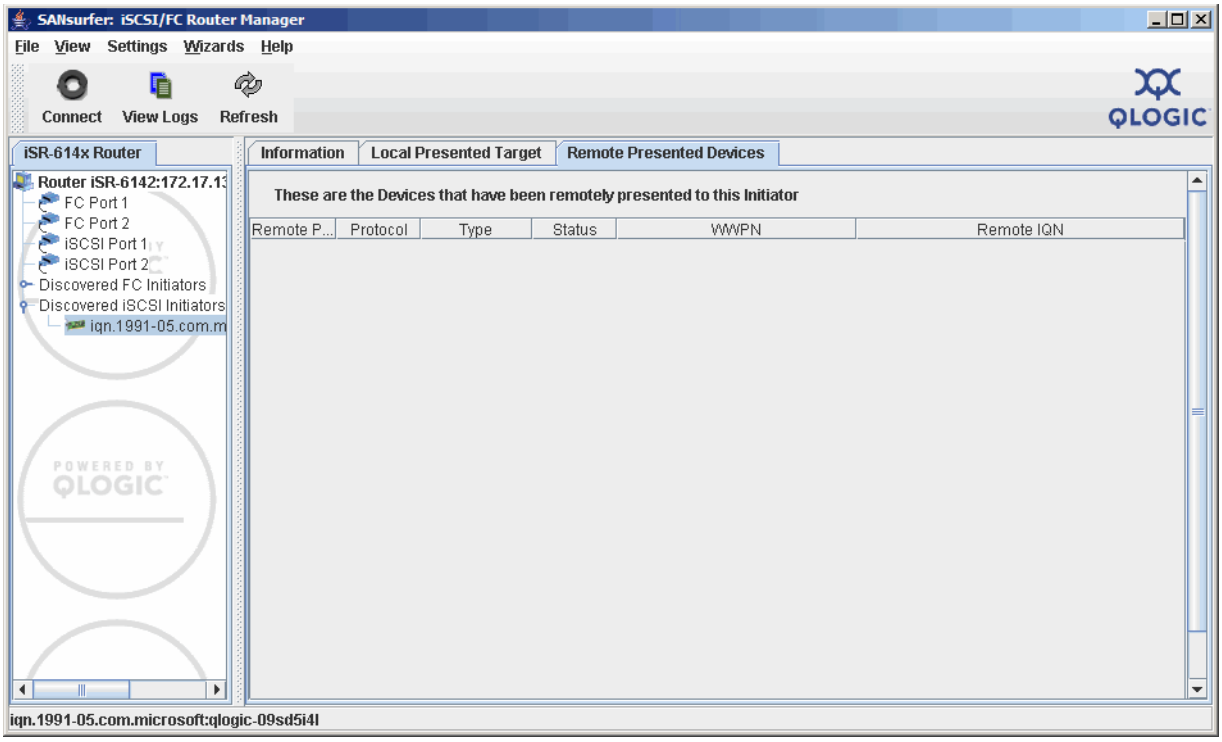

Figure 3-16 Remote Presented Target Tabbed Page

- **Remote Port** – Displays information provided by the target LUN in response to the router issuing a SCSI Inquiry command.
- **Protocol** – Displays information provided by the target LUN in response to the router issuing a SCSI Inquiry command.
- **Type** – Displays information provided by the target LUN in response to the router issuing a SCSI Inquiry command.

- **Status** – Displays information provided by the target LUN in response to the router issuing a SCSI Inquiry command.
- **WWPN** – Displays information provided by the target LUN in response to the router issuing a SCSI Inquiry command.
- **Remote IQN** – Displays information provided by the target LUN in response to the router issuing a SCSI Inquiry command.

FC Discovered Targets

Selecting an FC discovered target in the system tree does not provide any information in the right window. Select a discovered FC target to display the Information and Remote Presented Devices tabbed pages to the right of the system tree (see Figure 3-17).

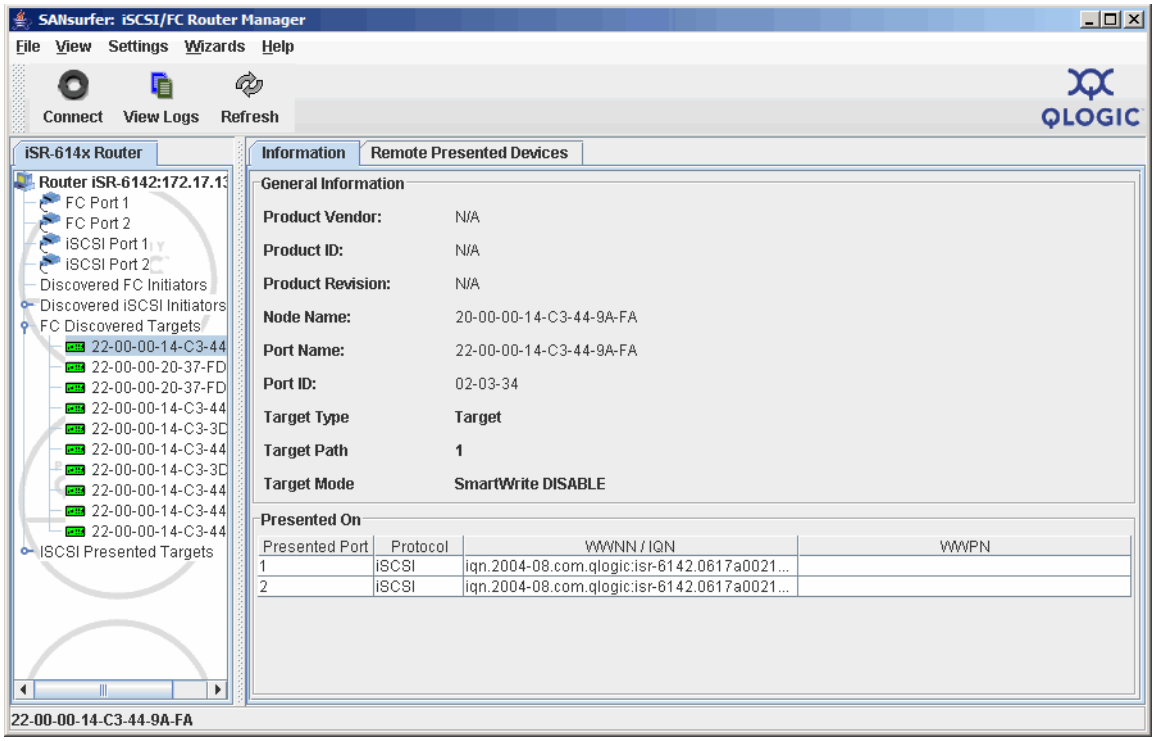

Figure 3-17 FC Discovered Targets Tabbed Pages

Information Tab

The Information tabbed page provides the following information about the selected FC target:

- **Product Vendor** – Displays the product vendor as reported by the SCSI Inquiry command.
- **Product ID** – Displays the product ID as reported by the SCSI Inquiry command.
- **Product Revision** – Displays the product revision as reported by the SCSI Inquiry command.
- **Node Name** – Displays the world-wide node name of the target device.
- **Port Name** – Displays the world-wide port name of the target device.
- **Port ID** – Displays the target device's port ID.

Remote Presented Devices Tab

The Remote Presented Devices tabbed page provides detailed target information and a scrollable list of LUNs, as shown in Figure 3-18 and described in the following paragraphs.

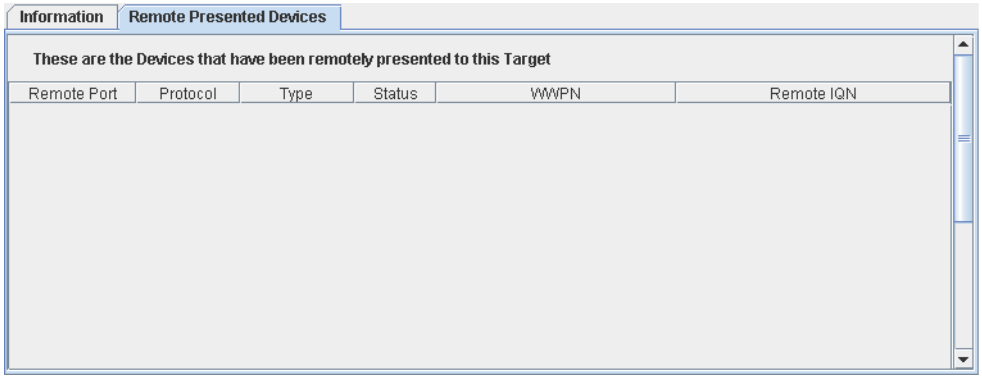

Figure 3-18 Remote Presented Devices Tab

- **General Information**
  - **Product Vendor** – Displays the vendor name of the target device as reported by the SCSI Inquiry command.
  - **Product ID** – Displays the product ID of the target device as reported by the SCSI Inquiry command.
  - **Product Revision** – Displays the product revision of the target device as reported by the SCSI Inquiry command.

- **Node Name** – Displays the world-wide node name of the target device.
- **Port Name** – Displays the world-wide port name of the target device.
- **Port ID** – Displays the target device's port ID.
- **Target Type** – Displays the FC port where the target device was discovered.
- **Target Path** – Displays the logical unit number.
- **Target Mode** – Displays the vendor name of the LUN as reported by the SCSI Inquiry command.

- **Remote Presented Devices** – Lists the devices that have been presented to this target as reported by the SCSI Inquiry command.

iSCSI Presented Target List Tabbed Page

The **iSCSI Presented Target List** tabbed page provides detailed FC target information and a scrollable list of the iSCSI presentations of the target, as shown in Figure 3-19 and described in the following paragraphs.

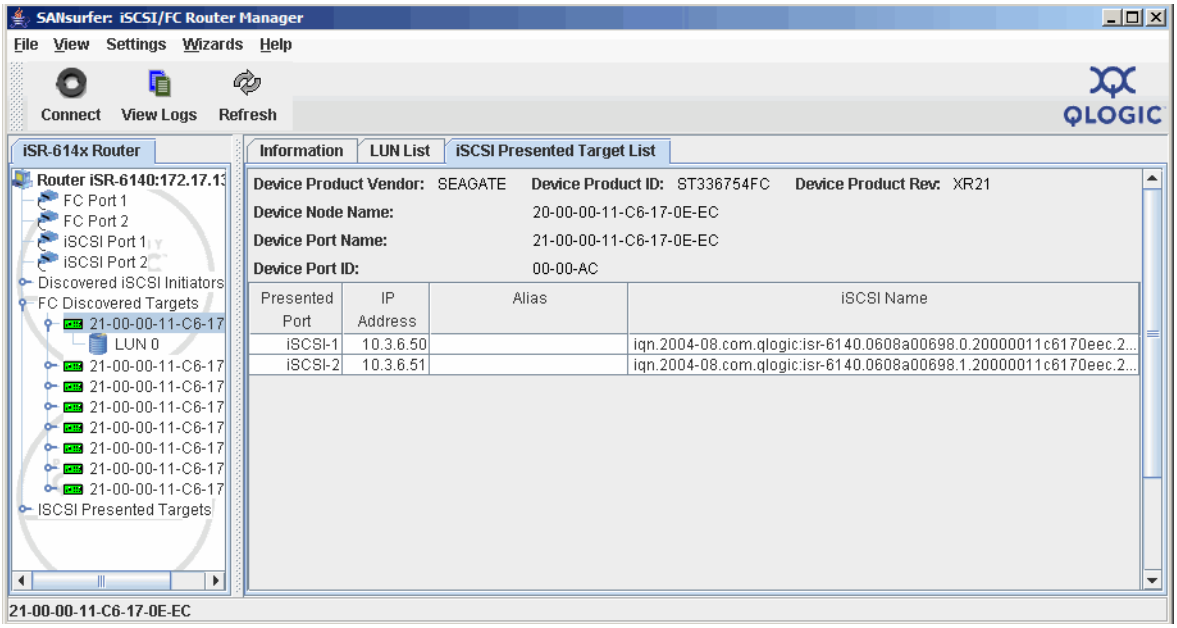

Figure 3-19 iSCSI Presented Target List Tabbed Page

- **Device Product Vendor** – Displays the vendor name of the target device as reported by the SCSI Inquiry command.
- **Device Product ID** – Displays the product ID name of the target device as reported by the SCSI Inquiry command.

- **Device Product Rev** – Displays the product revision of the target device as reported by the SCSI Inquiry command.
- **Device Node Name** – Displays the world-wide node name of the target device.
- **Device Port Name** – Displays the world-wide port name of the target device.
- **Device Port ID** – Displays the target device's port ID.
- **Presented Port** – Displays the iSCSI port number where the target is presented (1 or 2).
- **IP Address** – Displays the IP address on which the target is presented.
- **Alias** – Displays the iSCSI alias of the presented target.
- **iSCSI Name** – Displays the presented target's iSCSI name.
- **Size** – Displays the capacity (in megabytes) of the LUN as reported by the SCSI Capacity.

iSCSI Discovered Targets

The iSCSI Discovered Targets branch on the system tree does not provide any information in the right window. Select a discovered target to display the **Information** tabbed page to the right of the system tree (see Figure 3-20).

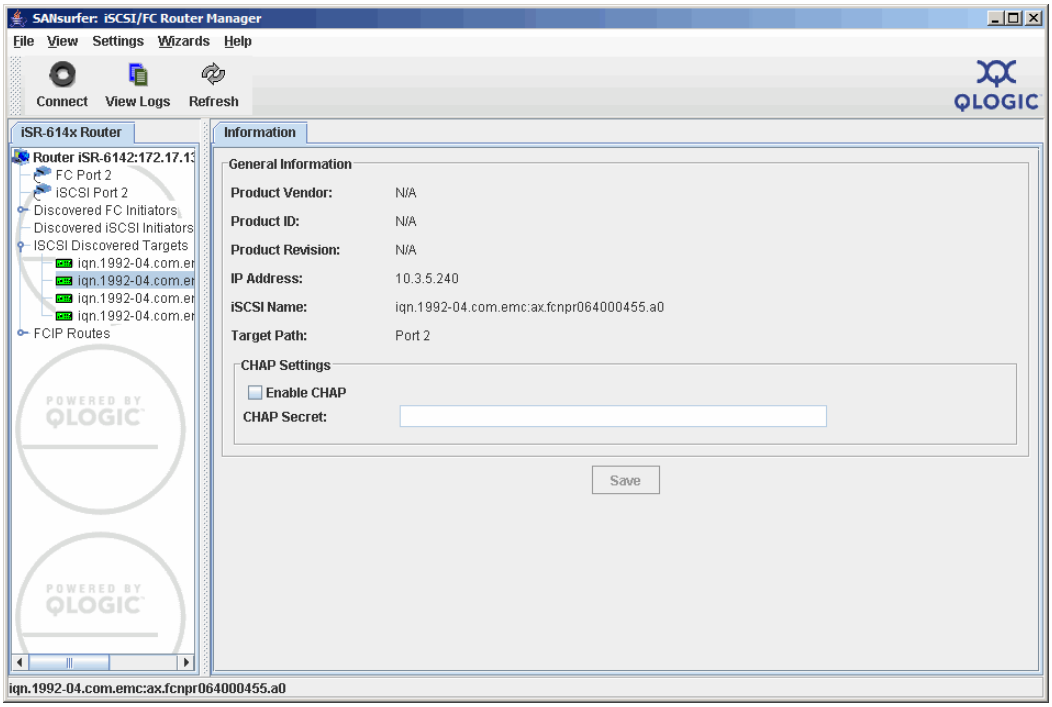

Figure 3-20 iSCSI Discovered Targets Tabbed Pages

Information Tabbed Page

The **Information** tabbed page consists of two sections: General Information and CHAP Settings, which are described in the following paragraphs.

- **General Information**
  - **Product Vendor** – Displays the product vendor as reported by the SCSI Inquiry command.
  - **Product ID** – Displays the product ID as reported by the SCSI Inquiry command.
  - **Product Revision** – Displays the product revision as reported by the SCSI Inquiry command.
  - **IP Address** – Displays the IP address of the presented iSCSI target.

- **iSCSI Name** – Displays the presented iSCSI target's name.
- **Target Path** – Displays the router's iSCSI port where the target was discovered.

- **CHAP Settings** – Provides an option you can use to set the challenge handshake authentication protocol (CHAP) option as follows:
  - **Enable CHAP** – Select this check box to enable CHAP when connecting to this target.
  - **CHAP Secret –** When the **Enable CHAP** option is enabled, you can enter the string used for the CHAP secret when connecting to this target.

NOTE:

If you change the **CHAP Settings**, you must click **Save** for the change to take effect.

FCIP Routes

Selecting the FCIP Routes branch on the system tree does not provide any information in the right window. Select an **FCIP Route Info #** in the system tree to display the branch to display the **FCIP Route Information** and **Statistics** tabbed pages to the right of the system tree.

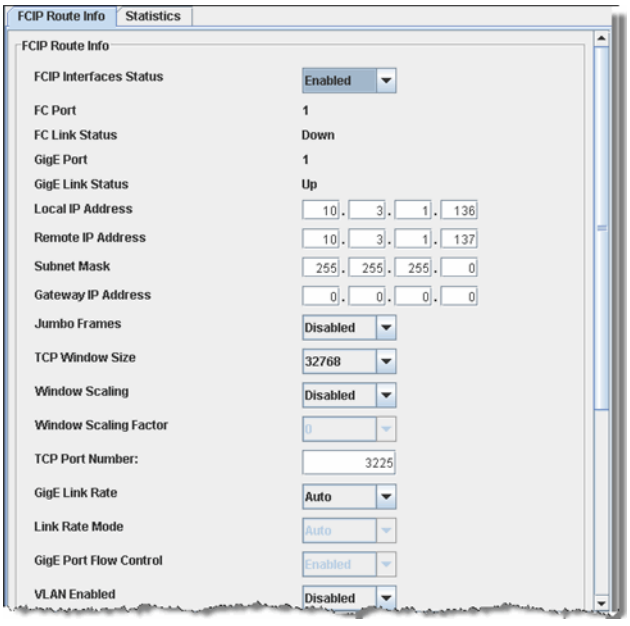

Figure 3-21 FCIP Route Tabbed Pages

FCIP Route Information Tabbed Page

The FCIP Route Information tabbed page contains the information that defines the selected FCIP route, as described in the following paragraphs.

- **FCIP Interface Status** – Provides a drop-down box you can use to enable or disable the FCIP route. Disabling the route places the FC and GE ports in a down state, but still retains all route configuration parameters.
- **FC Port** – Identifies the FC port assigned to the FCIP route when it was created.
- **FC Link Status** – Shows the state of the FC port used in this FCIP route.
- **GigE Port** – Identifies the gigabit Ethernet (GigE) port assigned to the FCIP route when it was created.
- **GigE Link Status** – Shows the state of the GigE port used in this FCIP route.
- **Local IP Address** – Fields you can use to define the IP address to be used by the GigE port. An uninitialized port has an IP address of all zeros.
- **Remote IP Address** – Fields you can use to define the IP address of the GigE port on the remote router.
- **Subnet Mask** – Fields you can use to define the subnet mask used by the GigE port.
- **Gateway IP Address** – Fields you can use to define the gateway IP address used by the GigE port.
- **Jumbo Frames** – Provides a drop-down box you can use to enable or disable Jumbo IP frames. When disabled, the MTU is 1500 bytes; when enabled, the maximum MTU is 9000 bytes.

  NOTE:

  Jumbo Frames should only be used with 1000 Mbps Ethernet networks.

- **TCP Window Size** – Provides a drop-down box you can use to choose one of three options for TCP window size: **8192**, **16384**, or **32768** bytes. The default is **32768**.
- **Window Scaling** – Provides a drop-down box you can use to enable or disable TCP window scaling. The default is disabled.
- **Window Scaling Factor** – When **Window Scaling** is enabled, use this drop-down box to choose one of six options for TCP window scaling: **0**–**5**.
- **TCP Port Number** – Field you can use to define the TCP port number.

- **GigE Link Rate** – Provides a drop-down box from which you can choose the link rate of the GigE port from one of four options: **Auto**, **10 Mbps**, **100 Mbps**, or **1000 Mbps**.
- **Link Rate Mode** – When the GigE Link Rate is set to something other than auto, use this drop-down box to choose one of three options for the link rate mode: **Auto**, **Half Duplex**, or **Full Duplex**.
- **GigE Port Flow Control** – When the GigE Link Rate is set to something other than **Auto**, use this drop-down box to enable or disable GigE port flow control. The default is enabled.
- **VLAN Enabled** – Provides a drop-down box you can use to enable or disable VLAN support. The default is disabled.
- **VLAN ID** – When VLAN is enabled, use this field to define the VLAN ID. The VLAN ID must be the same on both routers participating in the FCIP route (local and remote routers must be using same VLAN ID) and the Ethernet switches.
- **VLAN Priority** – When VLAN is enabled, use this drop-down box to set the VLAN priority to one of eight options: **0** through **7**.
- **Error Detect Timeout** – Provides a drop-down box you can use to set the error detect timeout value by selecting one of five options: **1** to **5** seconds. The default is one second.
- **Resource Allocate Timeout** – Provides a drop-down box you can use to set the resource allocate timeout value to one of five options: **1** to **5** seconds. The default is one second.
- **FCIP Timestamp** – Provides a drop-down box you can use to enable or disable FCIP timestamps. The default is enabled.
- **FCIP SW Compression** – Provides a drop-down box you can use to enable or disable FCIP compression. The default is disabled.
- **Bandwidth (Mbit/sec)** – Use this field to define the maximum bandwidth (in megabits per second) the GigE port will use during transmits. The range of values supported is `1` to `1000` megabits per second. Use this setting to limit the bandwidth used by the FCIP route so it doesn't consume all the available link bandwidth. For example, if the slowest link in the WAN being used is a DS-3 link, then the maximum available bandwidth is `45` megabits per second. To limit the FCIP route to 33% of the overall link bandwidth, set the bandwidth to `15` megabits per second.

NOTE:

To apply any changes made to this screen, click the **Save** button, located at the bottom of window.

FCIP Route Statistics Tabbed Page

The Statistics tabbed page consists of a scrollable table of parameters and values.

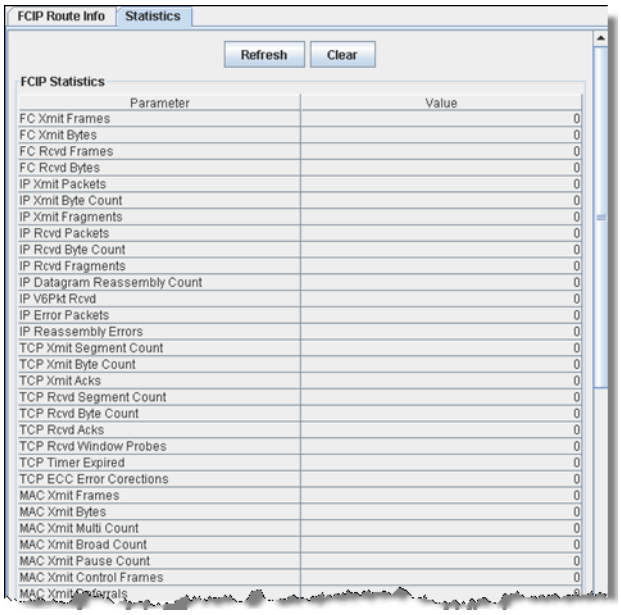

Figure 3-22 FCIP Route Statistics Page

You can refresh the statistics are by clicking **Refresh** at the top of the scrollable window. You can clear the statistics (set all values to zero) by clicking **Clear**.

Notes

4 Using the Wizards

The Router Manager provides easy-to-use wizards that walk you through various router configuration procedures.

The following topics describe how to use the available wizards:

- "Launching a Wizard" on page 4-1
- "Configuration Wizard" on page 4-2
- "Add Initiator Wizard" on page 4-7
- "FW Update Wizard" on page 4-9
- "Map Local Initiator/Target Wizard" on page 4-13
- "Unmap Local Initiator/Target Wizard" on page 4-20
- "Add Remote Router Wizard" on page 4-25
- "Remove Remote Router Wizard" on page 4-30
- "Map Remote Initiator/Target Wizard" on page 4-33
- "Remote Mapped Device" on page 4-39
- "Discover iSCSI Target Wizard" on page 4-42
- "FCIP Route Add Wizard" on page 4-45
- "FCIP Route Remove Wizard" on page 4-51

Launching a Wizard

You can launch an available wizard using any of the following methods:

- Select an option from the **Wizards** menu, located on the Router Manager's menu bar (see page 2-5.)
- Right-click anywhere within the router's node in tree window and select one of the wizards available from the action menu (see page 2-10.)
- If the router manager identifies unconfigured ports when you first connect to a router, it automatically launches the configuration wizard.

Configuration Wizard

The Configuration Wizard provides a set of dialog boxes that walk you through the steps required for configuring the iSCSI ports. This wizard starts automatically when your system connects to a system with any un-configured iSCSI ports.

You can also start this wizard at any time by selecting **Configuration Wizard** from the Wizards Menu or from the Action Menu.

After launching the Configuration Wizard, it displays the **iSCSI Port Selection** dialog box (see Figure 4-1).

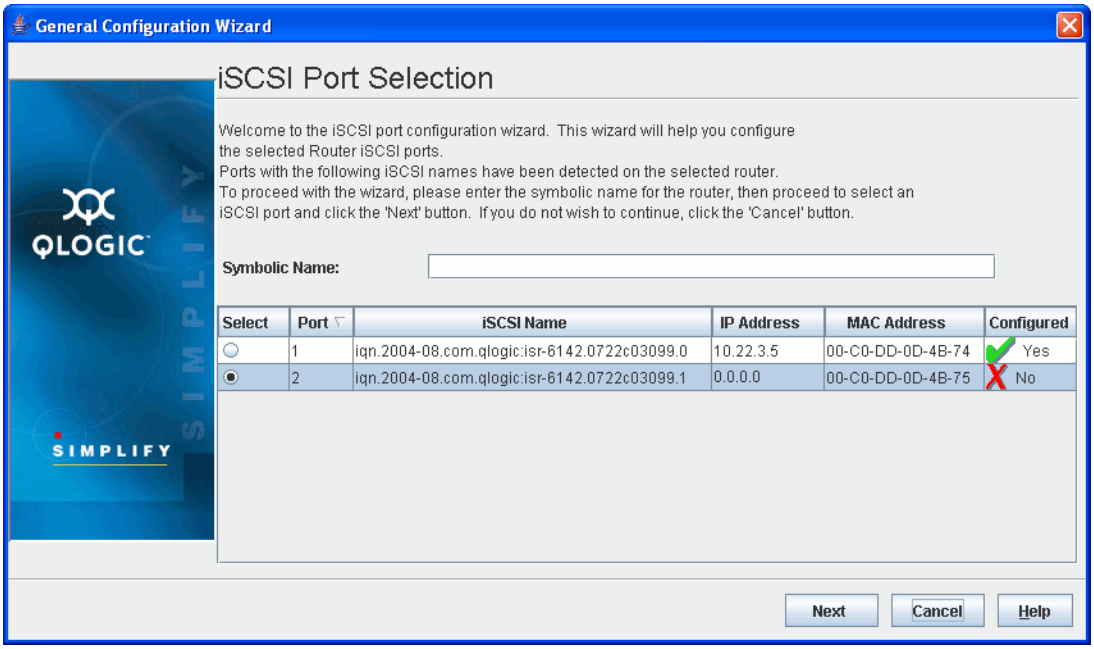

Figure 4-1 iSCSI Port Selection Dialog Box

To use the Configuration Wizard, follow these steps:

1. On the iSCSI Port Selection dialog box, select an unconfigured iSCSI port, enter the symbolic name for the router (if desired), then click **Next**.

   The **iSCSI Port Connection Settings Panel** dialog box displays (see Figure 4-2).

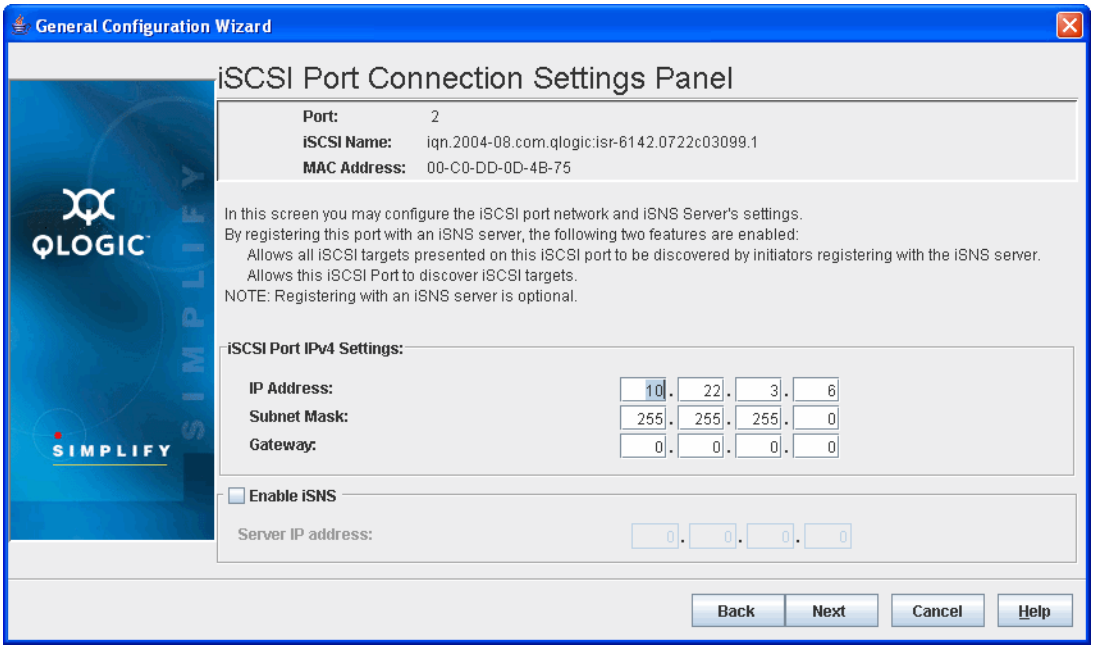
General Configuration Wizard
iSCSI Port Connection Settings Panel
Port: 2
iSCSI Name: iqn.2004-08.com.qlogic:isr-6142.0722c03099.1
MAC Address: 00-C0-DD-0D-4B-75
In this screen you may configure the iSCSI port network and iSNS Server's settings.
By registering this port with an iSNS server, the following two features are enabled:
Allows all iSCSI targets presented on this iSCSI port to be discovered by initiators registering with the iSNS server.
Allows this iSCSI Port to discover iSCSI targets.
NOTE: Registering with an iSNS server is optional.
iSCSI Port IPv4 Settings:
IP Address: 10 . 22 . 3 . 6
Subnet Mask: 255 . 255 . 255 . 0
Gateway: 0 . 0 . 0 . 0
Enable iSNS
Server IP address: 0 . 0 . 0 . 0
QLOGIC
SIMPLIFY
Back
Next
Cancel
Help

Figure 4-2 iSCSI Port Connection Settings Panel Dialog Box

2. To configure the iSCSI Port IPV4 settings:
   a. Type the information in the following fields.
      - **IP Address**
      - **Subnet Mask**
      - **Gateway**
   b. If desired, configure the IP address of the iSNS server with which the router registers the selected iSCSI port:
      - Select the **Enable iSNS** check box to make the **Server IP address** field editable.
      - Enter the IP address of the iSNS server in the **Server IP address** field.
3. Click **Next**. The **iSCSI Port IPv6 Settings Panel** appears, as shown in **Figure 4-3**.

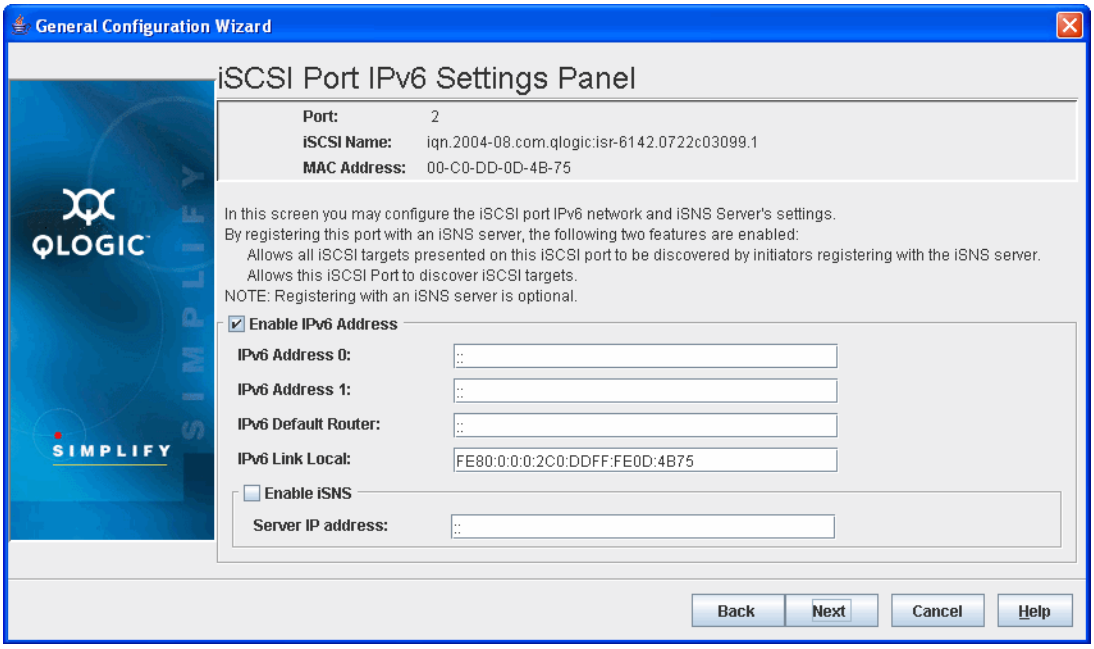
General Configuration Wizard
iSCSI Port IPv6 Settings Panel
Port: 2
iSCSI Name: iqn.2004-08.com.qlogic:isr-6142.0722c03099.1
MAC Address: 00-C0-DD-0D-4B-75
In this screen you may configure the iSCSI port IPv6 network and iSNS Server's settings.
By registering this port with an iSNS server, the following two features are enabled:
Allows all iSCSI targets presented on this iSCSI port to be discovered by initiators registering with the iSNS server.
Allows this iSCSI Port to discover iSCSI targets.
NOTE: Registering with an iSNS server is optional.
Enable IPv6 Address
IPv6 Address 0:
IPv6 Address 1:
IPv6 Default Router:
IPv6 Link Local:
FE80:0:0:0:2C0:DDFF:FE0D:4B75
Enable iSNS
Server IP address:
Back
Next
Cancel
Help
QLOGIC
SIMPLIFY

Figure 4-3 iSCSI Port IPv6 Settings Panel

4. To configure the iSCSI port IPv6 connection using this dialog box, follow these steps:
   a. Select **Enable IPv6 Address** to make the fields editable.
   b. Specify the iSCSI port IPv6 network settings:
      - Enter the **IPv6 Address 0**.
      - Enter the **IPv6 Address 1**.
      - Enter the **IPv6 Default Router**.
      - Enter the **IPv6 Link Local**.
   c. If desired, configure the IP address of the iSNS server with which the router registers the selected iSCSI port:
      - Select the **Enable iSNS** check box to make the **Server IP address** field editable.
      - Enter the IP address of the iSNS server in the **Server IP address** field.
5. Click **Next**. The Confirm Changes dialog box displays, as shown in Figure 4-4.

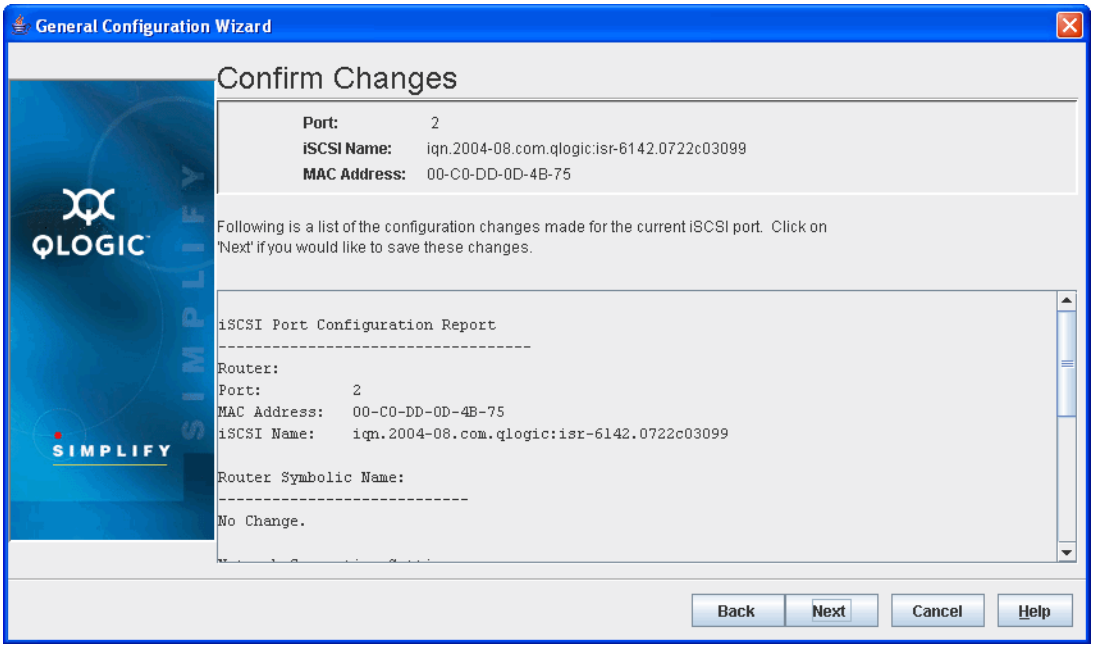

Figure 4-4 Confirm Changes Dialog Box

6. Review the configuration changes displayed on the screen, then click **Next** to confirm your changes.

The system displays the **iSCSI Port Configuration Status** dialog box, as shown in Figure 4-5.

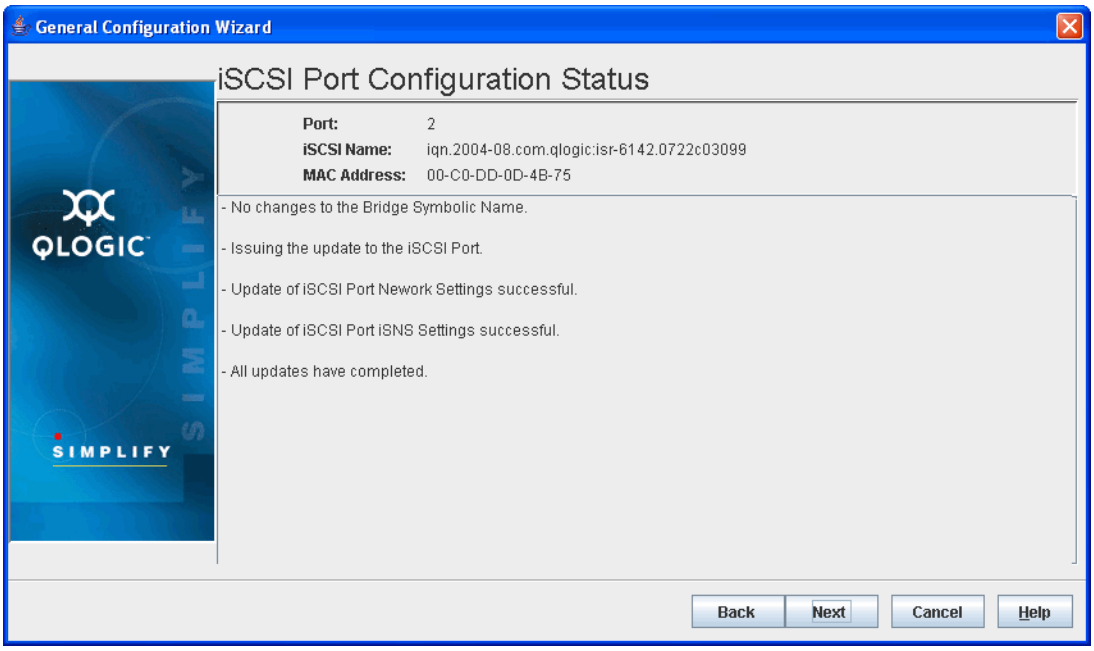

Figure 4-5 iSCSI Port Configuration Status

7. Read the information about the status changes, then click **Next**.

   The system displays the **Refresh** dialog box.

8. Read the information. If you would like to see the new configuration, click **Yes**; otherwise, click **No**.

   The system displays the **Finish** dialog box, as shown in Figure 4-6.

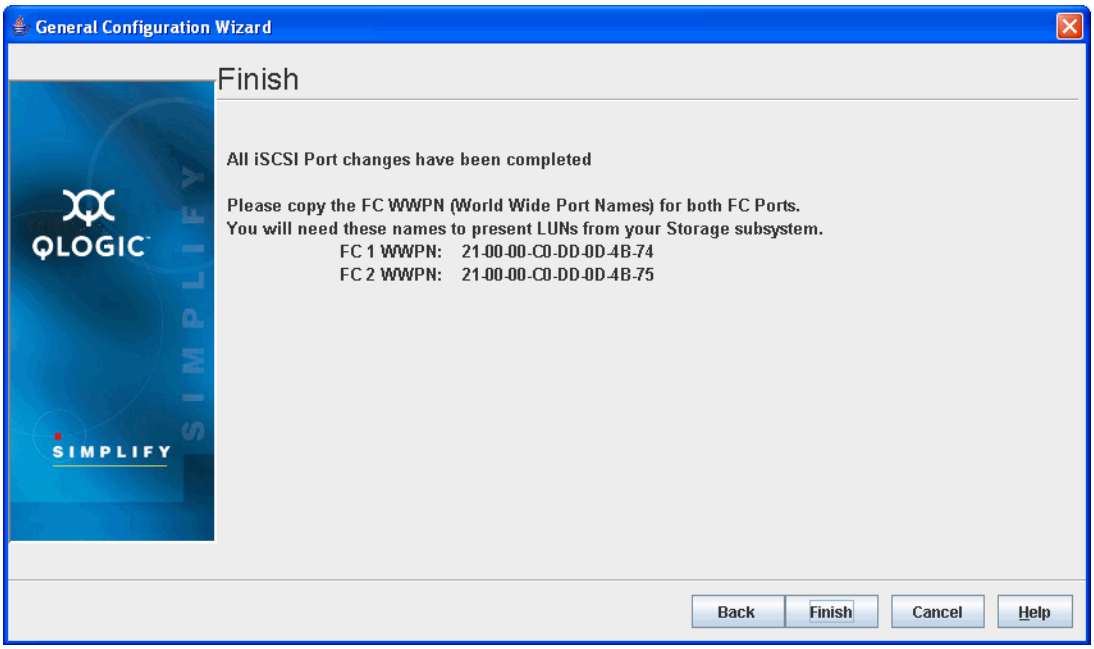

Figure 4-6 Configuration Wizard Finish Dialog Box

9. Read the information, then click **Finish**.

Add Initiator Wizard

The Add Initiator Wizard provides a dialog box used to enter an iSCSI initiator into the system database. iSCSI initiators are normally discovered (their name and address are captured) the first time they log in to the iSR6142 router.

This wizard allows you to enter the initiator information before the log in, thus allowing you to map LUNs to the initiator before logging into the iSR6142.

You can also start this wizard at any time by selecting **Add Initiator Wizard** from the Wizards Menu or from the Action Menu.

After launching the Configuration Wizard, the system displays the **iSCSI Port Selection** dialog box, as shown in Figure 4-7.

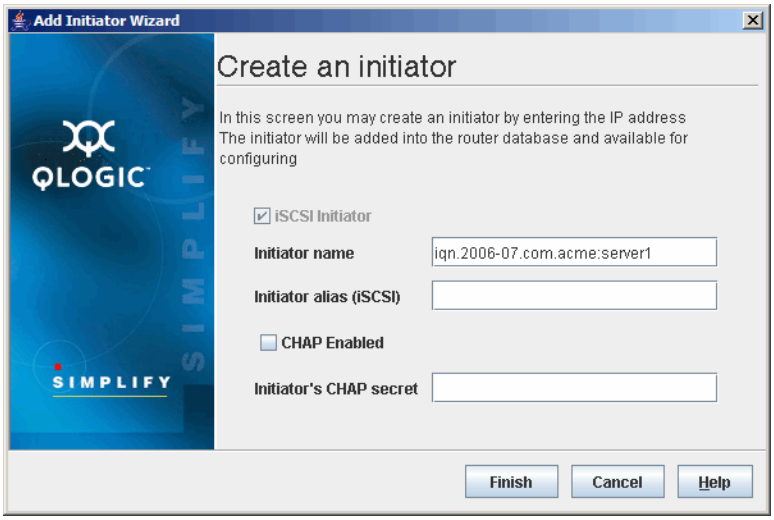

Figure 4-7 Create an Initiator Dialog Box

To create an initiator:

1. Type a name in the **Initiator name** box.
2. Type an alias in the **Initiator alias (iSCSI)** box.
3. If you want to enable CHAP for this initiator, select the **CHAP Enabled** check box. If you want a CHAP secret, type the name in the Initiator's **CHAP Secret** box.
4. Click **Finish**. The **Security Check** dialog box displays, as shown in Figure 4-8.

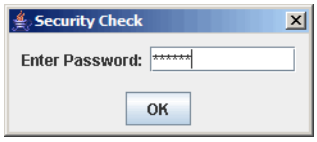

Figure 4-8 Security Check Dialog Box

5. Type the appropriate password, then click **OK**.

The new iSCSI initiator is displayed in the discovered iSCSI initiator's section of the system tree, as shown in Figure 4-9.

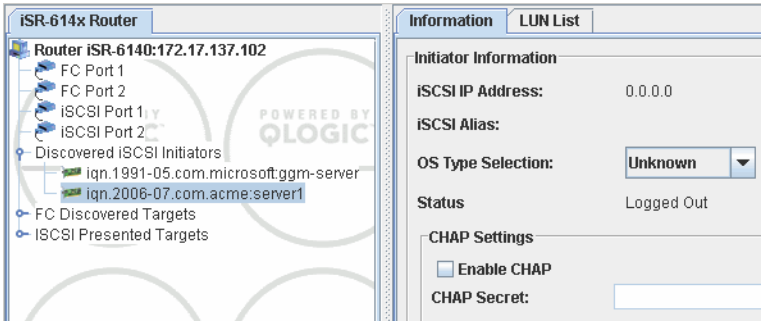

Figure 4-9 System Tree with New iSCSI Initiator

FW Update Wizard

The FW Update Wizard provides a set of dialog boxes that walk you through the steps required for updating the iSR6142 firmware. This wizard helps you update the firmware on selected router. When you first launch this wizard, the Router Selection dialog box displays all detected routers, as shown in Figure 4-10.

You can start this wizard at any time by selecting **FW Update Wizard** from the Wizards Menu or from the Action Menu.

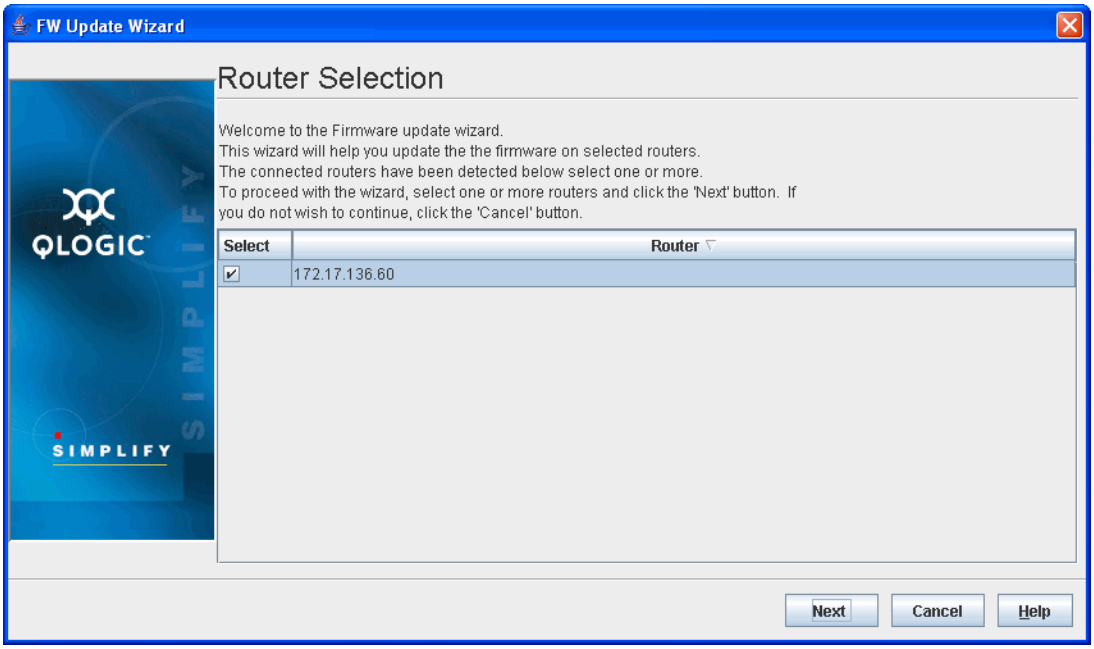
FW Update Wizard
Router Selection
Welcome to the Firmware update wizard.
This wizard will help you update the the firmware on selected routers.
The connected routers have been detected below select one or more.
To proceed with the wizard, select one or more routers and click the 'Next' button. If
you do not wish to continue, click the 'Cancel' button.
Select
Router
172.17.136.60
Next
Cancel
Help
SIMPLIFY

Figure 4-10 Router Selection Dialog Box

To update the firmware, follow these steps:

1. Select the check box next to the routers whose firmware you want to update, then click **Next**. The **Open** dialog box displays.

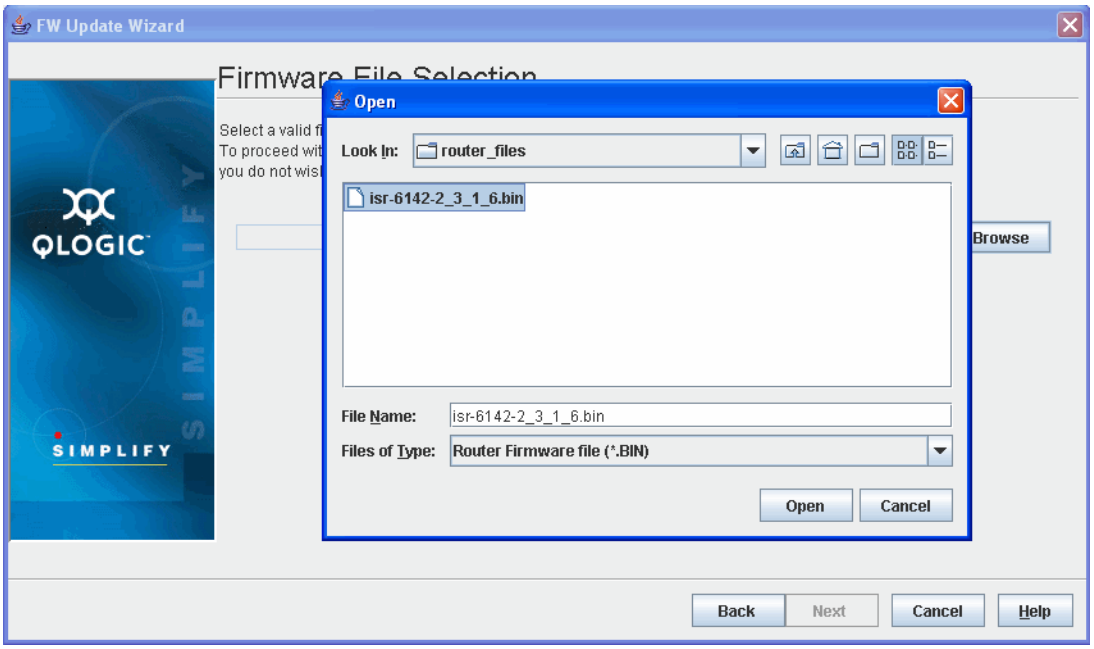

Figure 4-11 Firmware File Selection Dialog Box

2. Enter in the path to the firmware file, or click **Browse** to locate the firmware file.
3. When the firmware file is displayed in the **Firmware Image File** field, click **Next**.

The **Confirm Changes** dialog box displays, as shown in Figure 4-12.

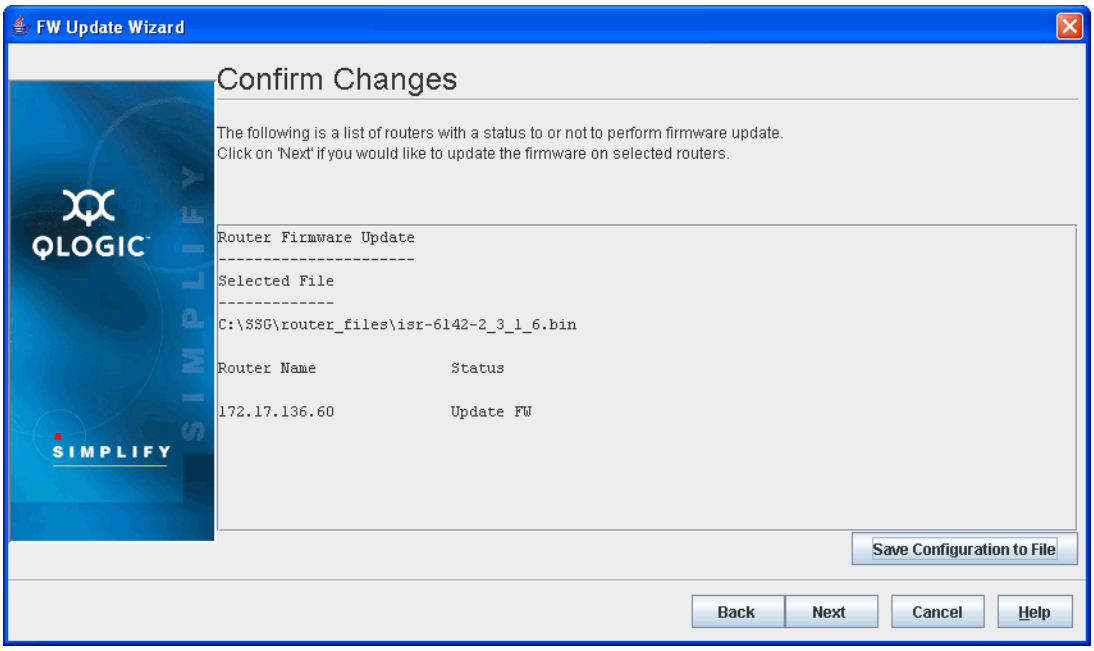

Figure 4-12 Confirm Changes Dialog Box

4. Read the information, then do the following:

   a. If you want to save a copy of this firmware configuration, click **Save Configuration to File**. Browse to the desired directory, type a file name, then click **Save**.

   b. Click **Next**. The **Security Check** dialog box requests the Admin password, as shown in Figure 4-13.

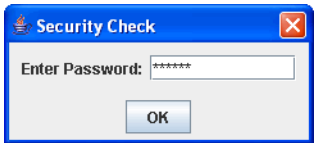

Figure 4-13 Security Check Dialog Box

   c. Type the appropriate password, then click **OK** to start the firmware update.

5. The **Firmware Update Status** dialog box shows the progress of the update in the message section, as shown in Figure 4-14.

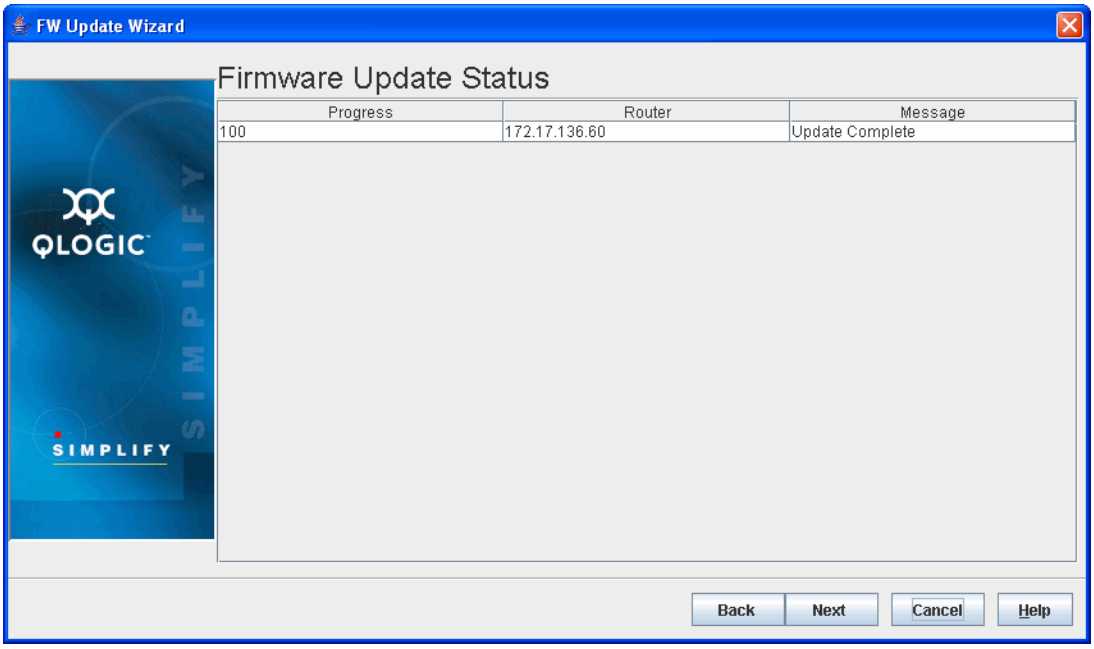

Figure 4-14 Firmware Update Status Dialog Box—Progress

When the firmware has loaded successfully, the system displays the **Finish** dialog box, along with the **Update success** dialog box, as shown in Figure 4-15.

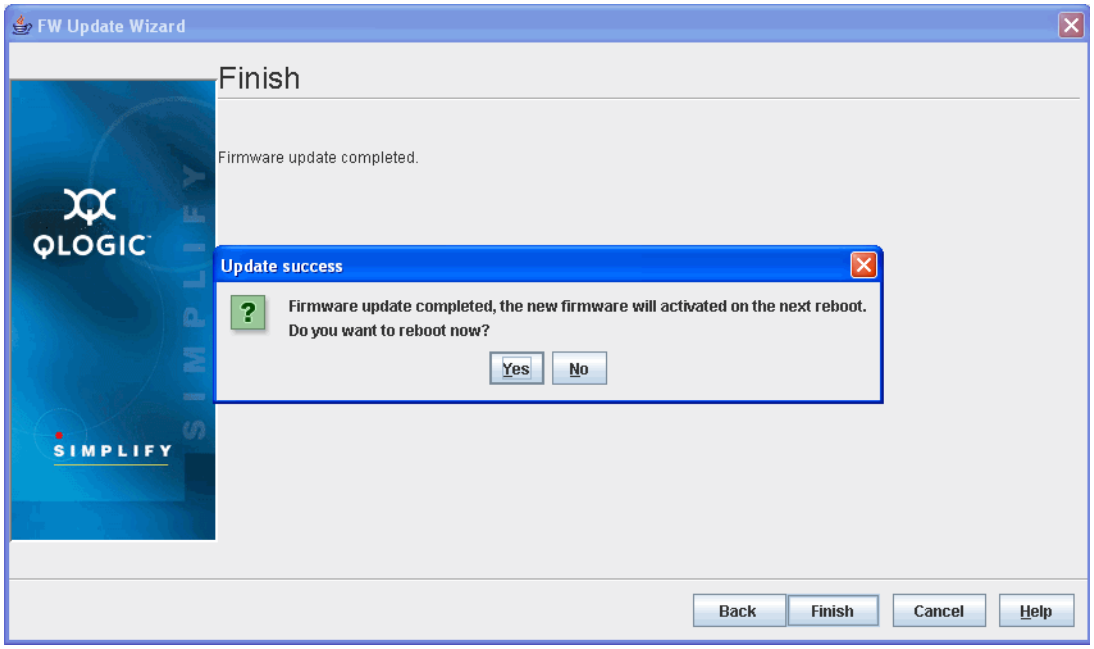

Figure 4-15 Finish Dialog Box (Successful Firmware Update)

NOTE:

The new firmware will not take effect until the system is rebooted.

6. Complete the wizard:
   a. If you want to reboot the system now, click **Yes**. Otherwise, click **No**.
   b. Click **Finish**.

Map Local Initiator/Target Wizard

The Map Local Initiator/Target Wizard provides a set of dialog boxes that walk you through the steps required for mapping a local initiator to a local target.

You can start this wizard at any time by selecting **Map Local Initiator/Target Wizard** from the Wizards Menu or from the Action Menu.

When the Map Local Initiator/Target wizard launches, the **Select an Initiator** dialog box displays a list of locally connected initiators (FC or iSCSI), as shown in Figure 4-16.

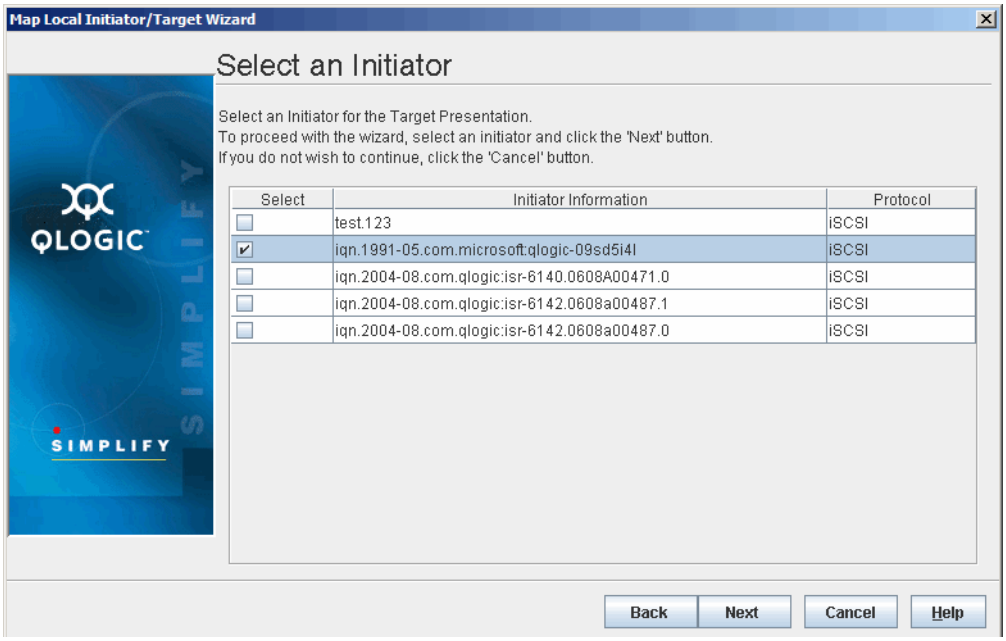

Figure 4-16 Initiator Selection Dialog Box

To map a local target to a local initiator:

1. Select the check box next to the initiator you want to map, then click **Next**.

The **Select a Target** dialog box opens, as shown in Figure 4-17.

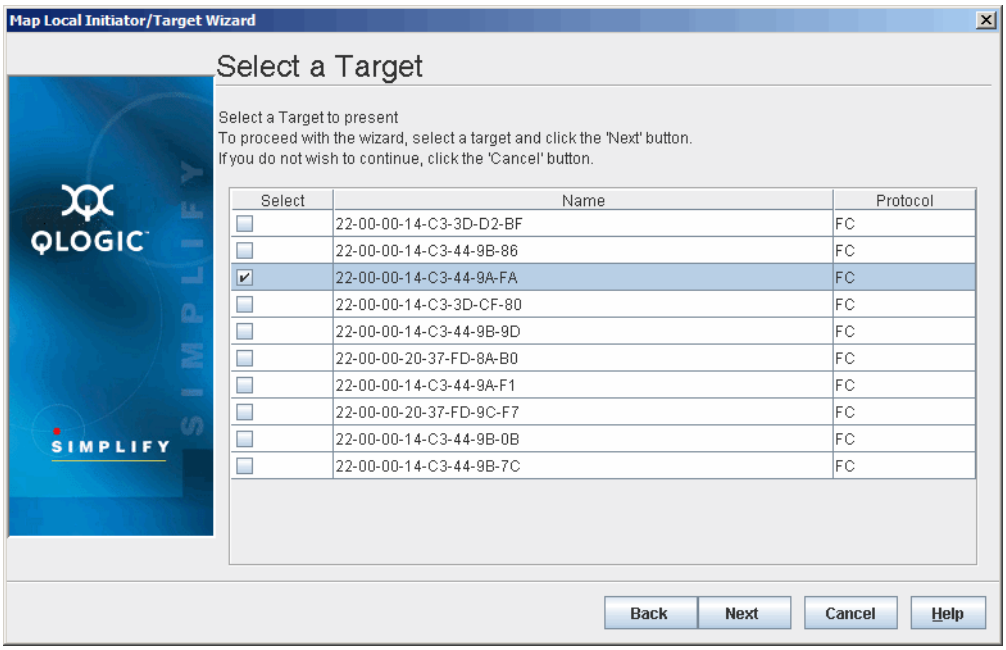

Figure 4-17 Select a Target Dialog Box

2. Select a target you want mapped to the previously selected initiator, then click **Next**.

The wizard screen prompts you to select a port on which the initiator will be presented, as shown in Figure 4-18.

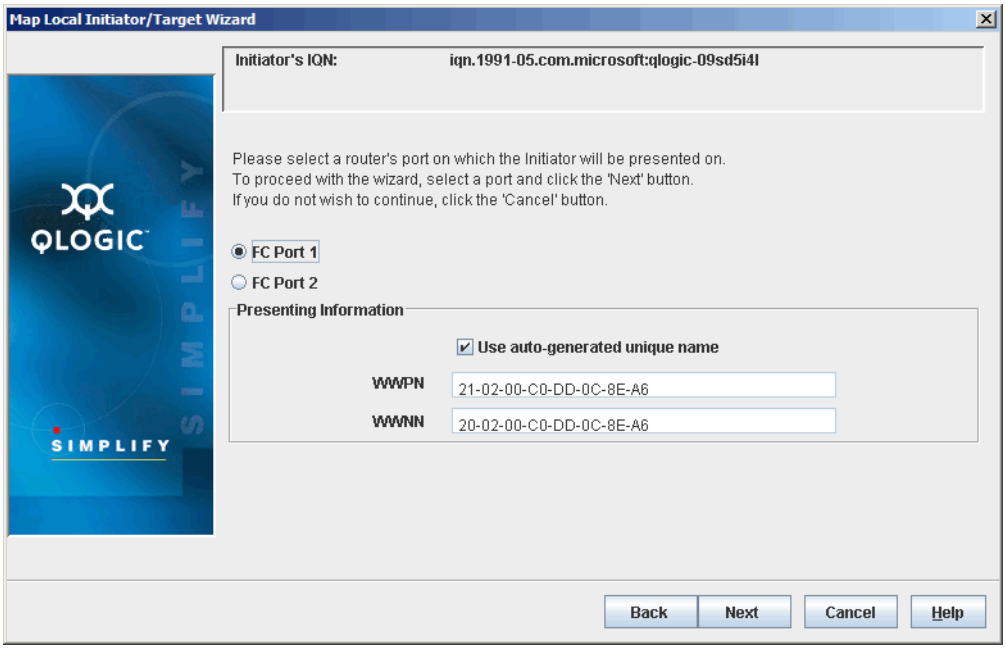

Figure 4-18 Select Initiator Port Dialog Box

3. Select the port (FC Port 1 or FC Port 2), then click **Next**.

The wizard screen prompts you to select a port on which the target will be presents (iSCSI Port 1 and iSCSI Port 2), as shown in Figure 4-19.

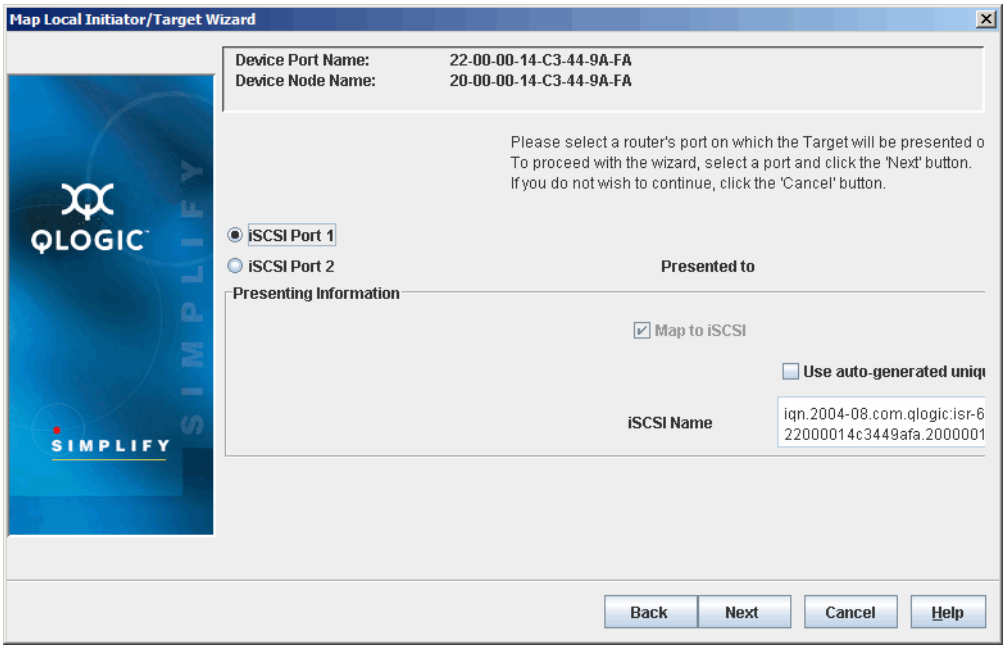

Figure 4-19 Select Target Presentation Port Dialog Box

The **Confirm Changes** dialog box displays the local mapping done in the previous steps, as shown in Figure 4-20.

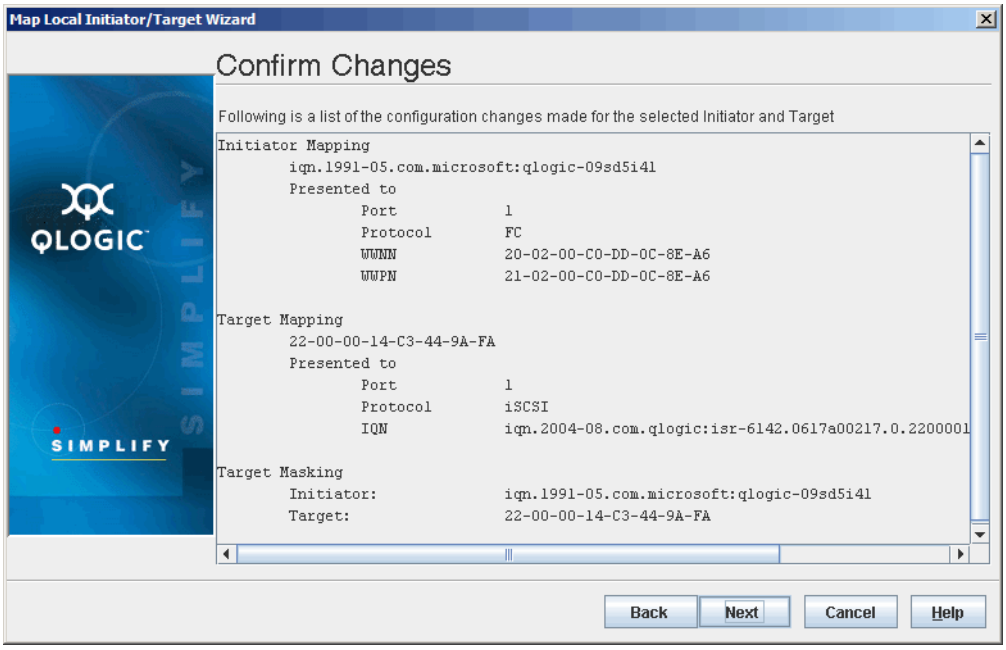

Figure 4-20 Confirm Changes Dialog Box

4. Review the information, then click **Next**.

The **Security Check** dialog box requests the Admin password, as shown in Figure 4-21.

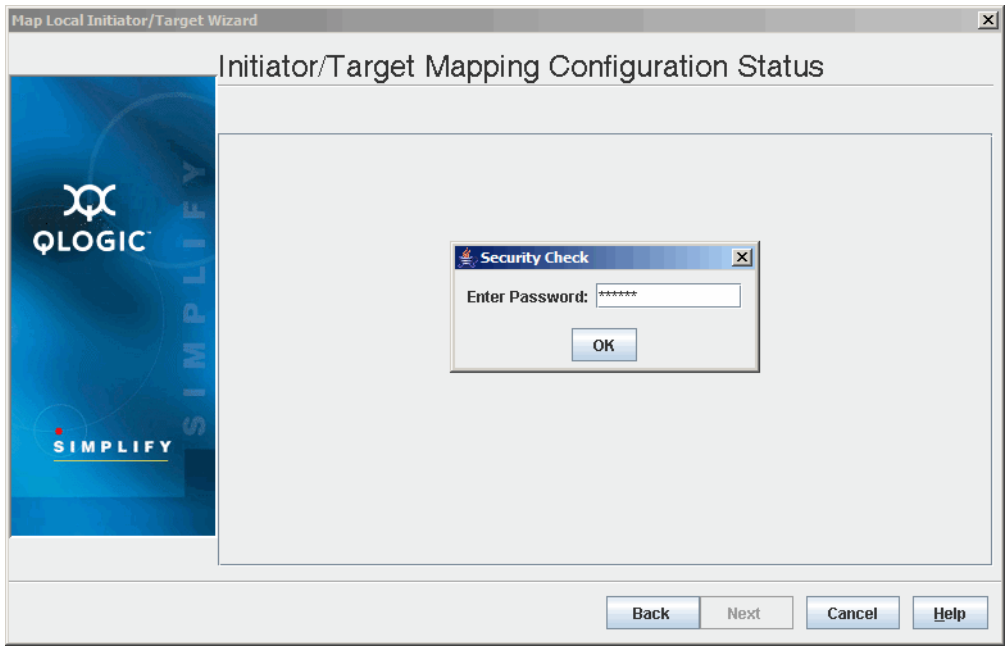

Figure 4-21 Security Check Dialog Box

5. Type the appropriate password, then click **OK** to confirm the local mapping.

The **Initiator/Target Mapping Configuration Status** dialog box displays local mapping completion status, as shown in Figure 4-22.

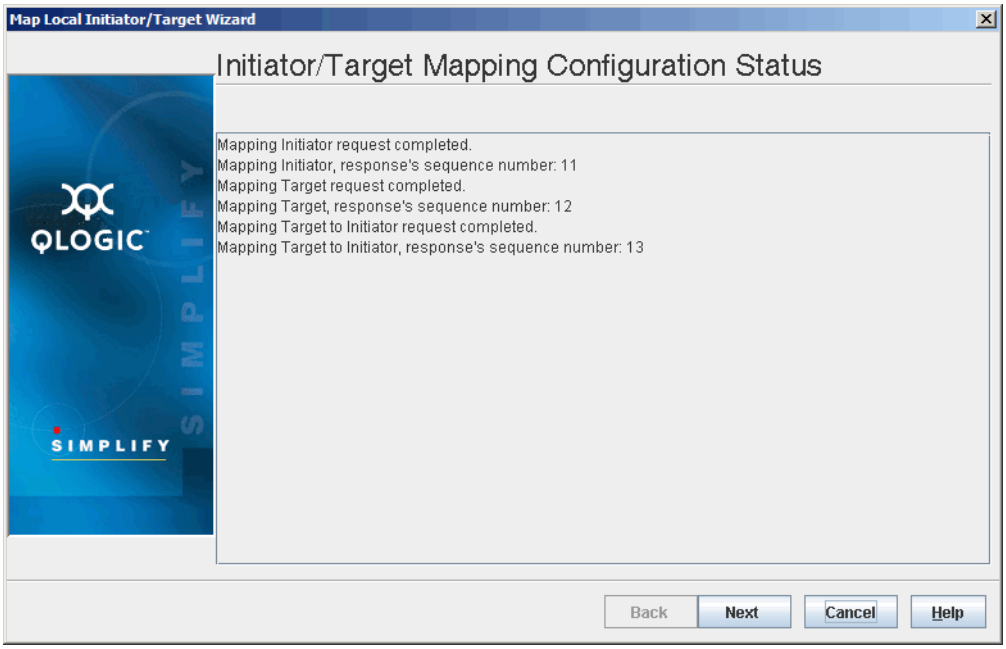

Figure 4-22 Initiator/Target Mapping Configuration Status Dialog Box

6. After reviewing the initiator to target mapping configuration status, click **Next**.

After completing the Map Local Initiator/Target Wizard, you can see the mapping by selecting the mapped Initiator in the system tree under **Discovered iSCSI Initiators**. Click the **Local Presented Devices** tab, as shown in Figure 4-23. In this example an iSCSI initiator is mapped to an FC target, other mappings are supported such as FC to FC, FC to iSCSI and iSCSI to iSCSI.

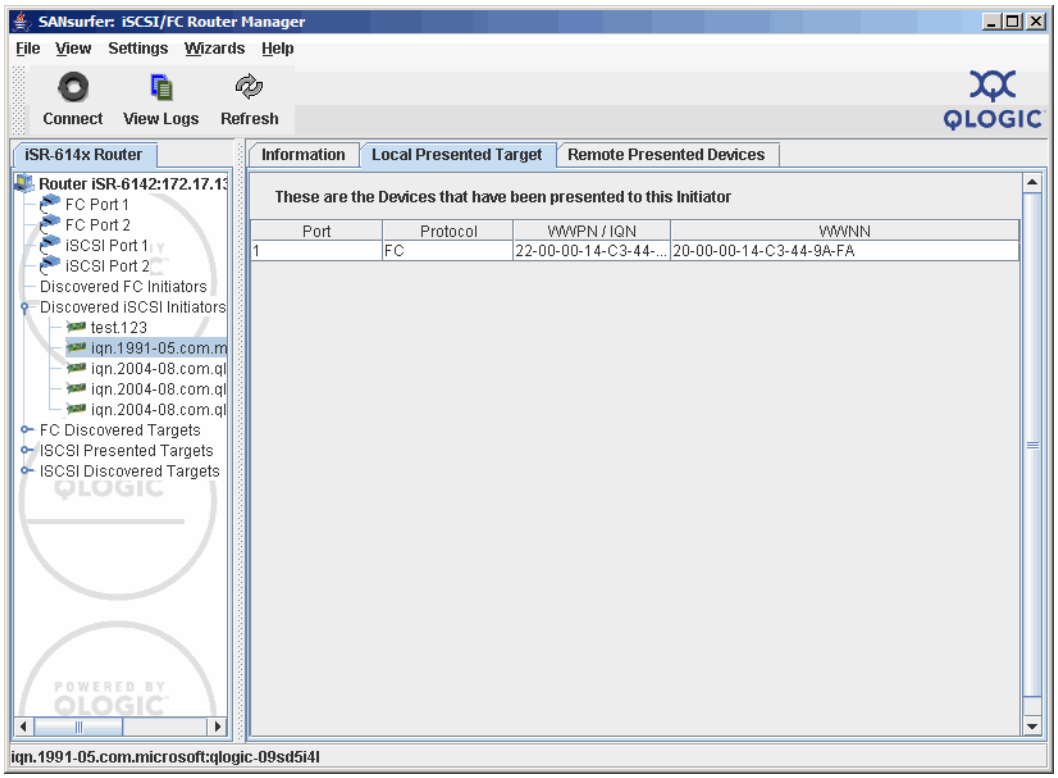

Figure 4-23 Discovered iSCSI Initiators - Local Presented Targets

Unmap Local Initiator/Target Wizard

The Unmap Local Initiator/Target Wizard provides a set of dialog boxes that walk you through the steps required for removing a local initiator from a local target mapping.

You can start this wizard at any time by selecting **Unmap Local Initiator/Target Wizard** from the Wizards Menu or from the Action Menu.

When the UnMap Local Initiator/Target Wizard launches, the **Select an Initiator** dialog box displays a list of locally connected initiators (FC or iSCSI), as shown in Figure 4-24.

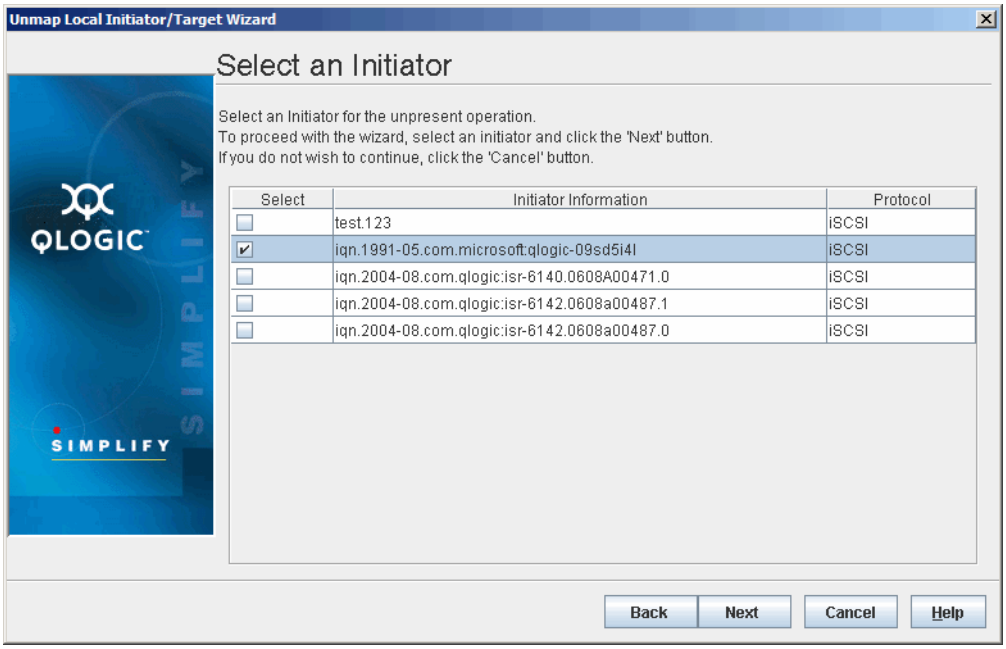

Figure 4-24 Initiator Selection Dialog Box

To unmap a local target from a local initiator:

1. Select the check box next to the initiator you want to unmap, then click **Next**.

The **Presented Target Selection** dialog box displays a list of targets mapped to the initiator selected in the previous step, as shown in Figure 4-25.

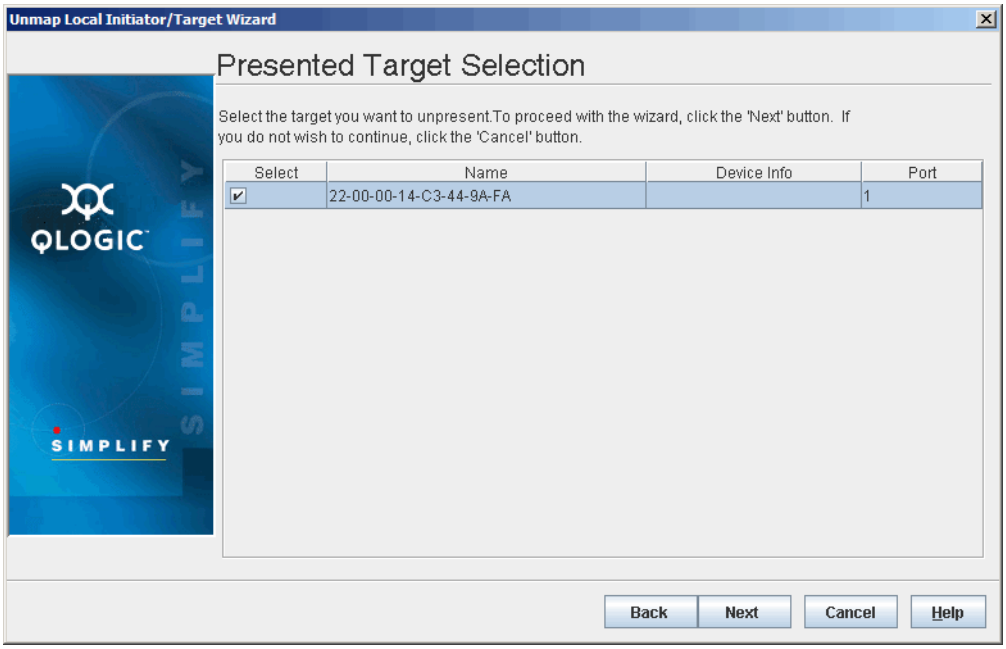

Figure 4-25 Presented Target Selection Dialog Box

2. Select the check box next to the target to unmap, then click **Next**.

The **Security Check** dialog box requests the Admin password, as shown in Figure 4-26.

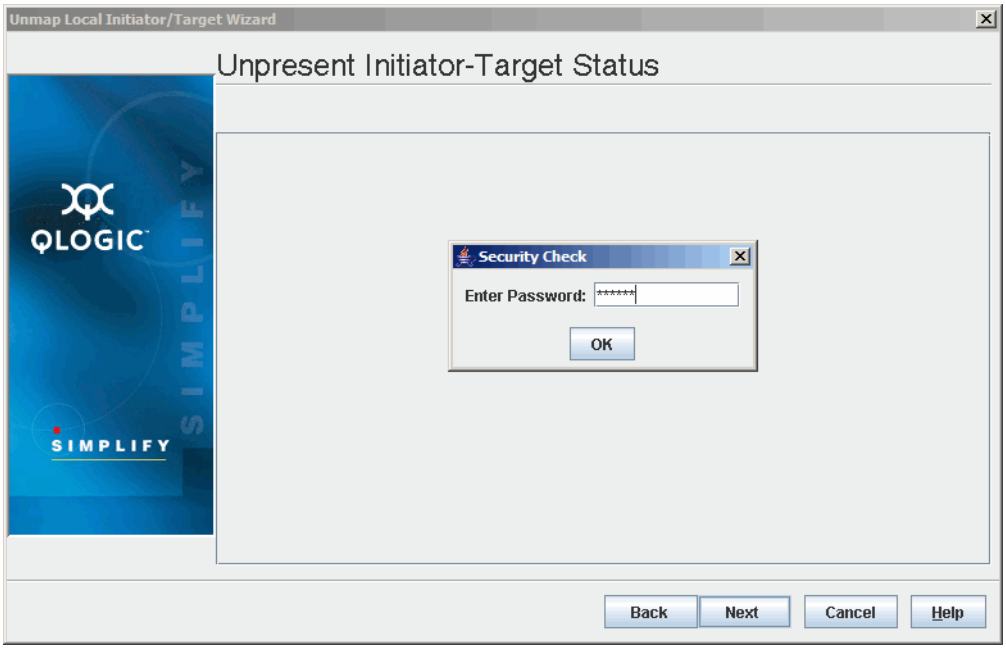

Figure 4-26 Security Check Dialog Box

3. Type the appropriate password, then click **OK** to confirm the target is unmapped.

The **Unpresent Initiator/Target Status** dialog box displays the results of the unmap operation, as shown in Figure 4-27.

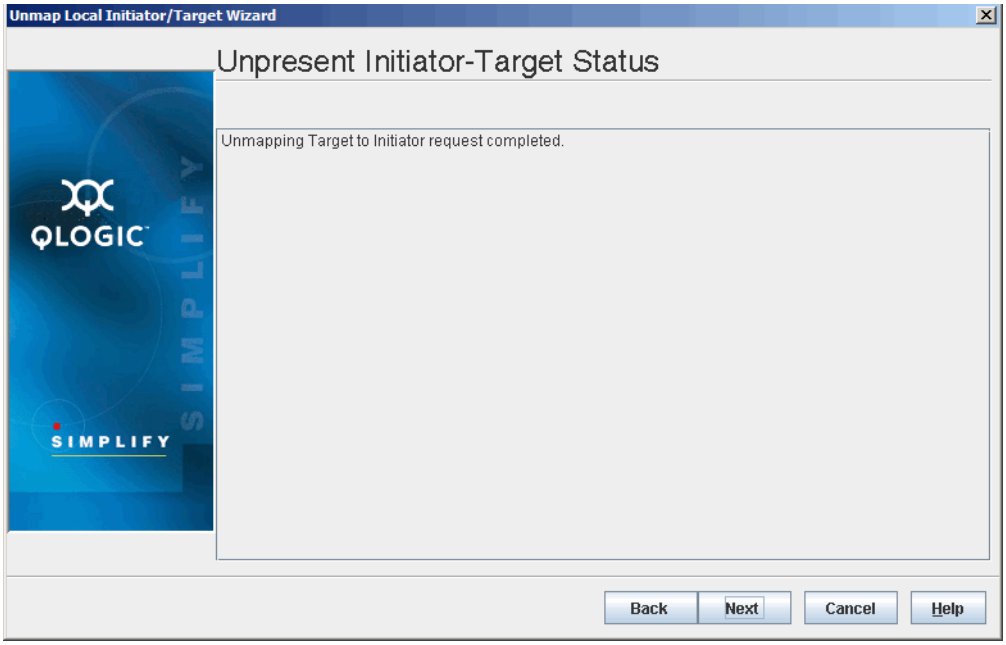

Figure 4-27 Unpresent Initiator/Target Status Dialog Box

4. Review the status, then click **Next**.

After completing the UnMap Local Initiator/Target Wizard you can verify the unmapping by selecting the Initiator in the system tree under **Discovered iSCSI Initiators.** Then select **Local Presented Devices**.

For the example shown in Figure 4-28, an iSCSI initiator was unmapped from an FC target.

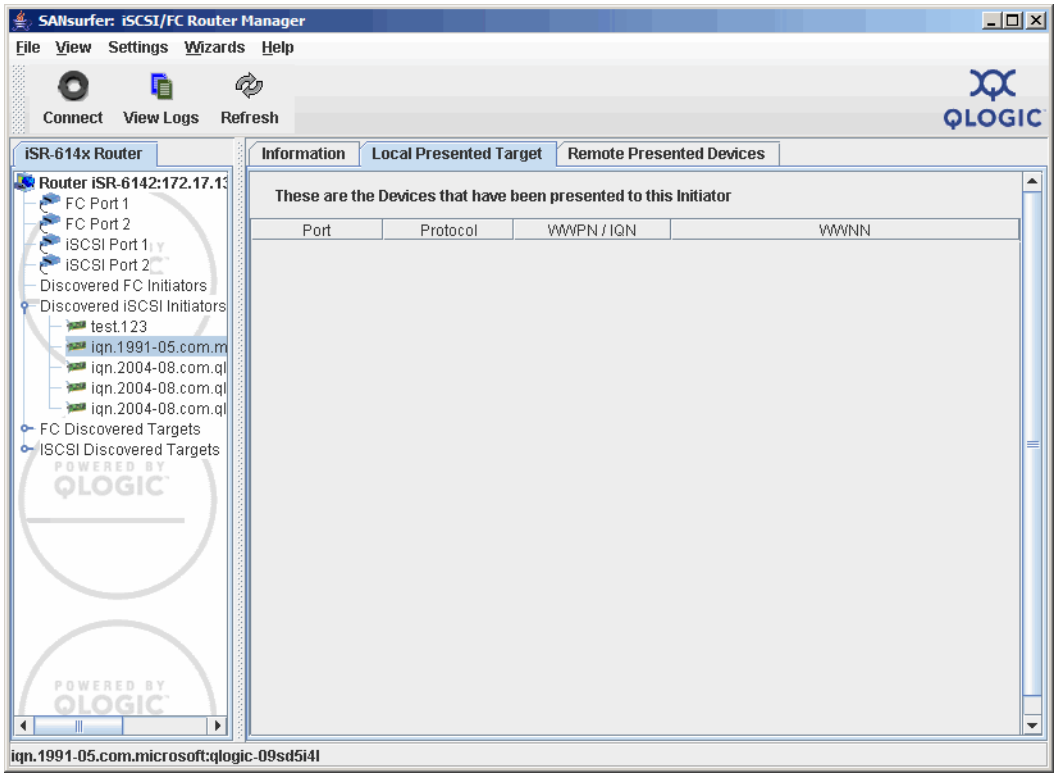

Figure 4-28 Discovered iSCSI Initiators - Local Presented Targets

Add Remote Router Wizard

The Add Remote Router Wizard provides a set of dialog boxes that walk you through the steps required for assigning a remote router to your local router as a peer.

You can start this wizard at any time by selecting **Add Remote Router Wizard** from the Wizards Menu or from the Action Menu.

When the Add Remote Router Wizard launches, the **Remote Router's IP Address** dialog box requests the remote router's IP address, as shown in Figure 4-29.

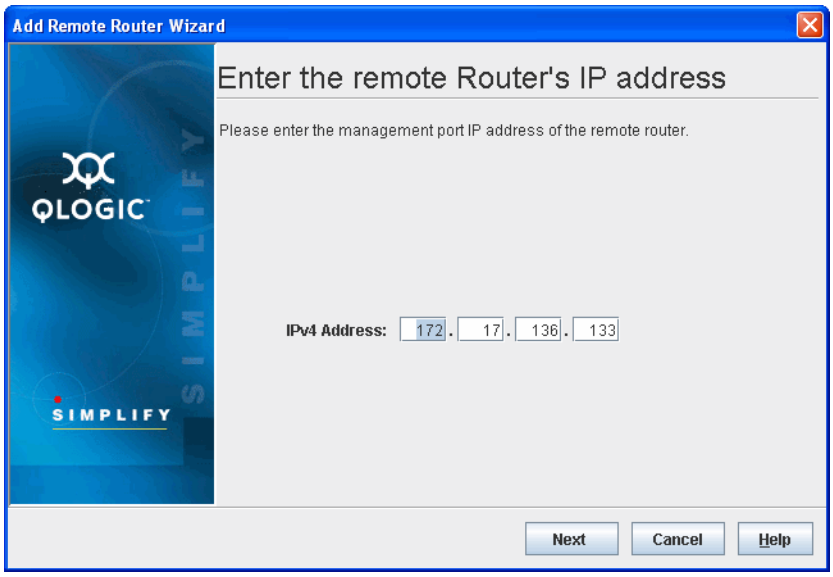

Figure 4-29 Remote Router's IP Address Dialog Box

To add a remoter router to a local router:

1. Type the IP Address of the remote router, then click **Next**.

The **Status** dialog box displays the remote router information along with the **Local Router Admin Password** dialog box, as shown in Figure 4-30.

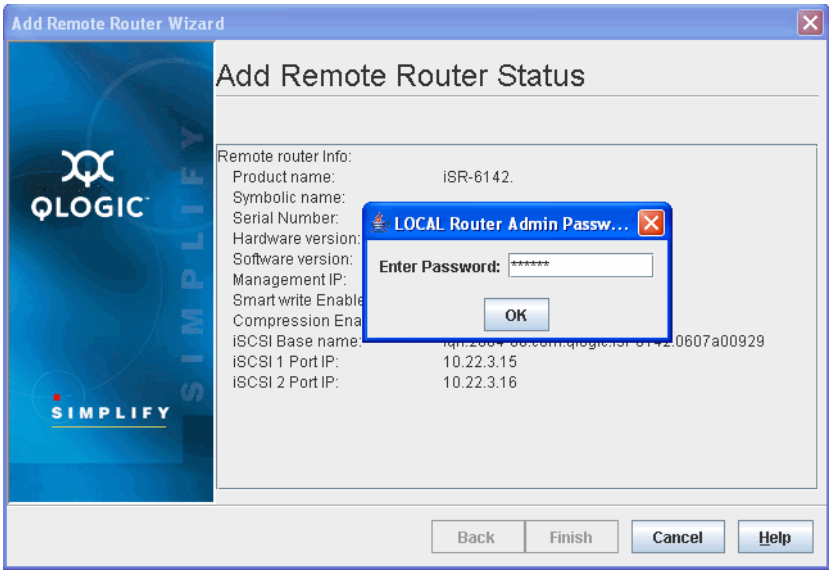

Figure 4-30 Local Router Admin Password Dialog Box

2. Type the local router admin password (default=config), then click **OK**.

   The **Status** dialog box displays the remote router information, as shown in Figure 4-31.

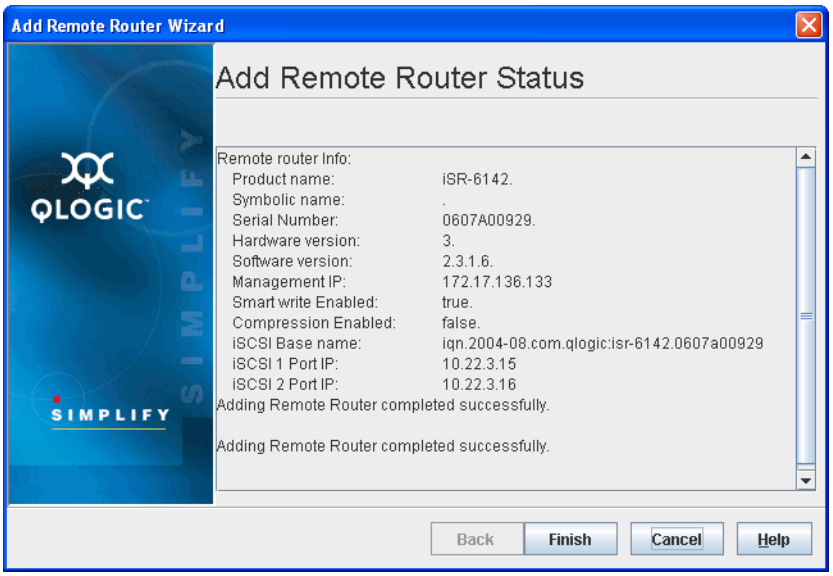

Figure 4-31 Add Remote Router Status Dialog Box

3. Review the status, then click **Finish**.
4. Click the **Refresh** icon to refresh the display.
5. Select the router node, then select the **Assigned Remote Router:1** tab to display the remote router's information, as shown in Figure 4-32.

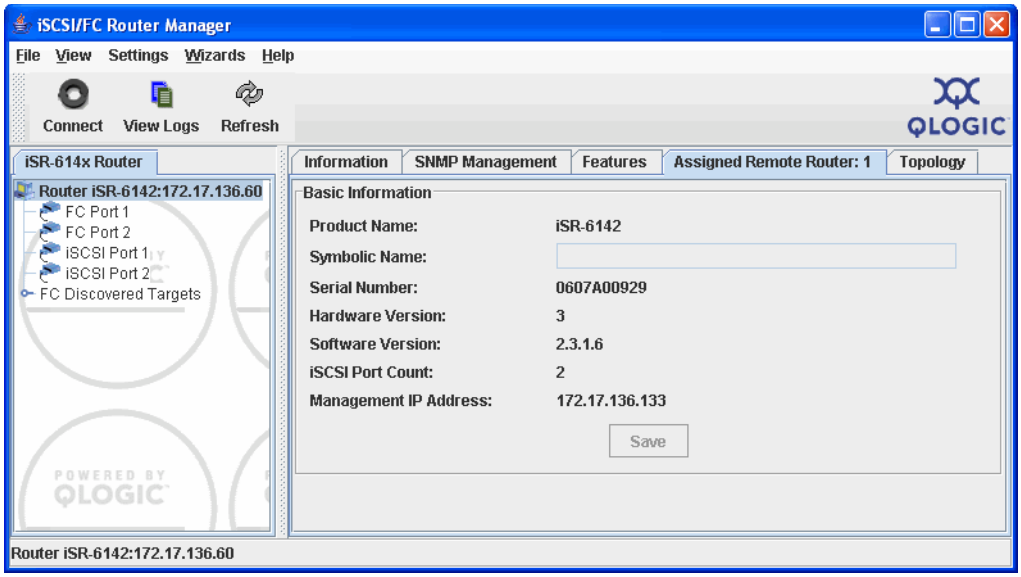

Figure 4-32 Assigned Remote Router Display

6. Click the **Topology** tab to display the local and remote router topology including devices attached to both routers, as shown in Figure 4-33.

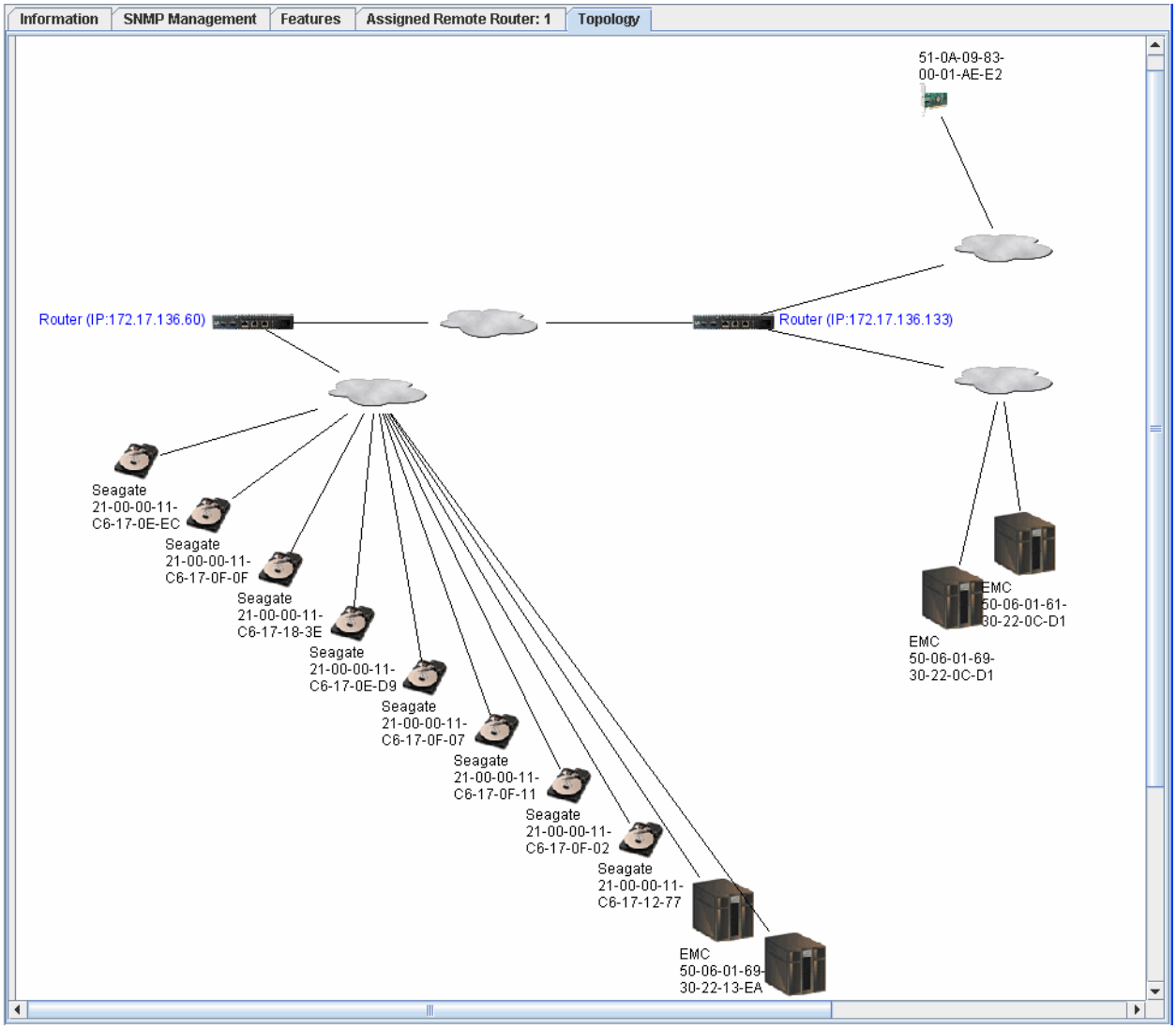

Figure 4-33 Topology Display

Remove Remote Router Wizard

The Remove Remote Router Wizard provides a set of dialog boxes that walk you through the steps required for removing a remote router from the local router.

You can start this wizard at any time by selecting **Remove Remote Router Wizard** from the Wizards Menu or from the Action Menu.

When the Remove Remote Router Wizard launches, the **Select a Remote Router to unmap** dialog box displays a list of mapped routers, as shown in Figure 4-34.

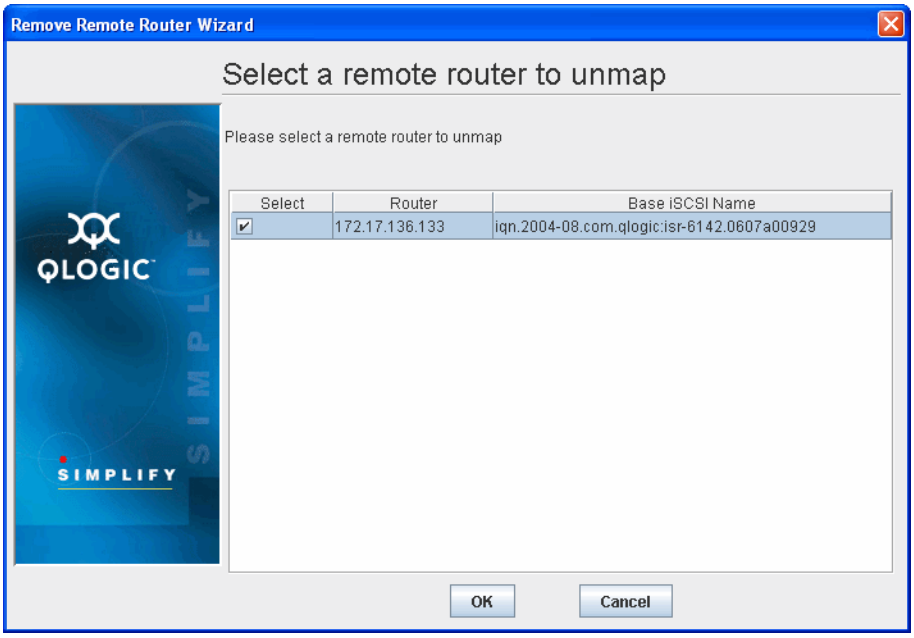

Figure 4-34 Select Remote Router Dialog Box

To remove a remoter router from a local router:

1. Select the remote router to be removed, then click **OK**.

The **Local Router Admin Password** dialog box requests the local router's admin password to complete the unmap, as shown in Figure 4-35.

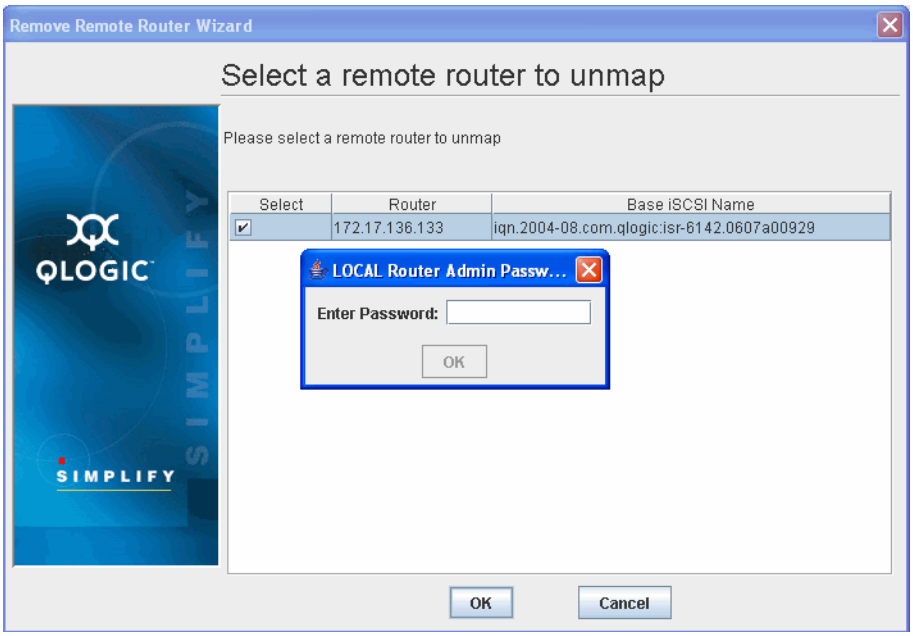

Figure 4-35 Local Router Admin Password Dialog Box

2. Type the local router's admin password (default=config), then click **OK**.

   The system prompts you to refresh the display, as shown in Figure 4-36.

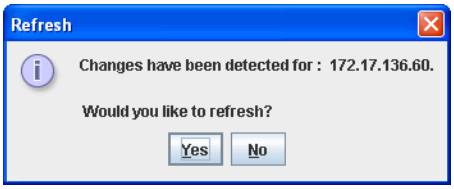

Figure 4-36 Refresh Screen

3. Click **Yes** to refresh the display.

The **Remove Remote Router Completion** dialog box displays the completion status, as shown in Figure 4-37.

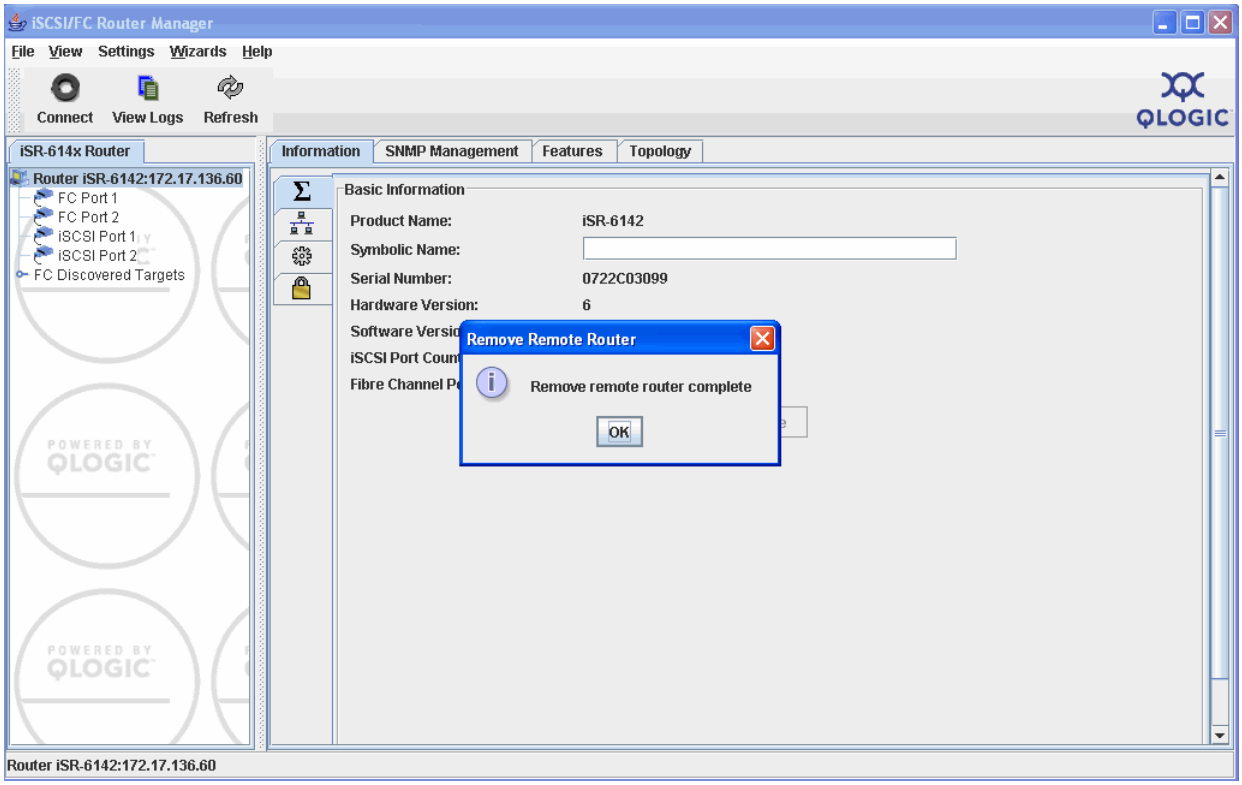

Figure 4-37 Remove Remote Router Completion Dialog Box

4. Click **OK** to close the message box.

Map Remote Initiator/Target Wizard

The Map Remote Initiator/Target Wizard provides a set of dialog boxes that walk you through the steps required for mapping an initiator to a target, one of which is remote and the other local.

You can start this wizard at any time by selecting **Map Remote Initiator/Target Wizard** from the Wizards Menu or from the Action Menu.

When the Map Remote Initiator/Target Wizard launches, the **Device Selection** dialog box displays a list of devices, as shown in Figure 4-38. If necessary, expand the router tree to see the attached devices.

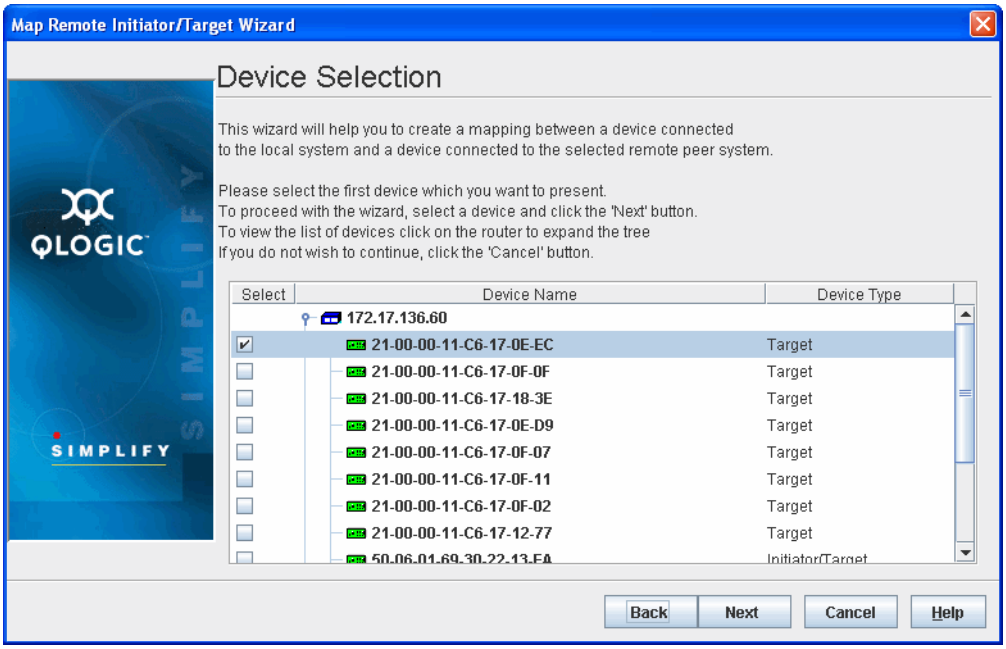

Figure 4-38 Device Selection Dialog Box

To create a remote-to-local mapping between an initiator to a target:

1. Select the device to be mapped. The device may be a target or an initiator and may be either on the remote router or on the local router.
2. Click **Next**.

The **Device Selection** dialog box displays list of devices, as shown in Figure 4-39.

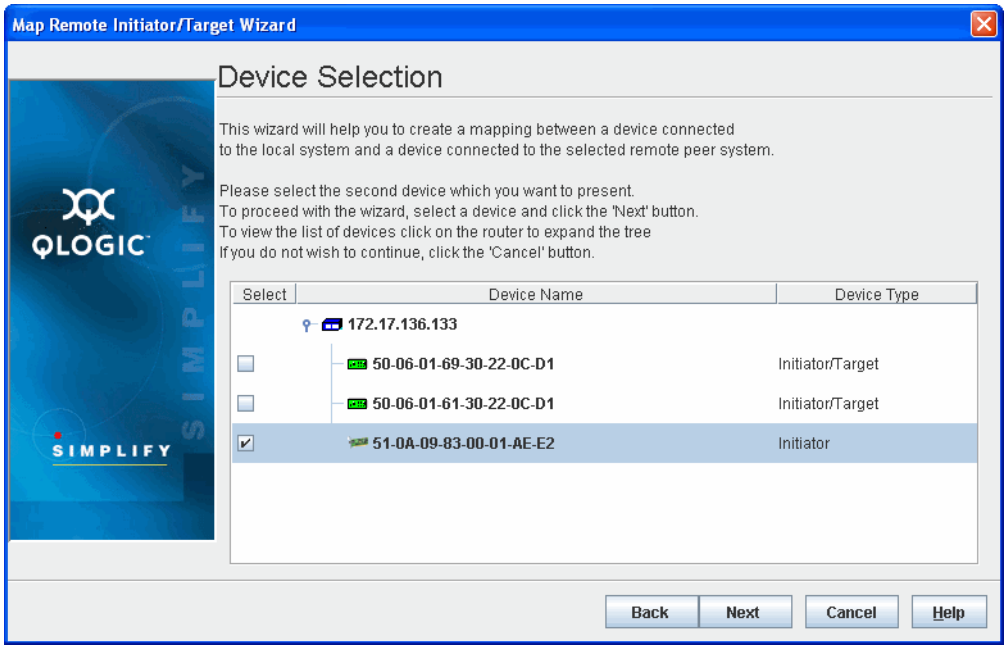
Map Remote Initiator/Target Wizard
Device Selection
This wizard will help you to create a mapping between a device connected
to the local system and a device connected to the selected remote peer system.
Please select the second device which you want to present.
To proceed with the wizard, select a device and click the 'Next' button.
To view the list of devices click on the router to expand the tree
If you do not wish to continue, click the 'Cancel' button.
Select
Device Name
Device Type
172.17.136.133
50-06-01-69-30-22-0C-D1
Initiator/Target
50-06-01-61-30-22-0C-D1
Initiator/Target
51-0A-09-83-00-01-AE-E2
Initiator
Back
Next
Cancel
Help
QLOGIC
SIMPLIFY

Figure 4-39 Device Selection Dialog Box

3. If necessary, expand the router tree to see the attached devices. Select the device to be mapped. The device may be a target or an initiator and may be on either the remote router or on the local router. Click **Next.**

The port selection dialog box prompts you to select a port the system will use to connect to the device, as shown in Figure 4-40.

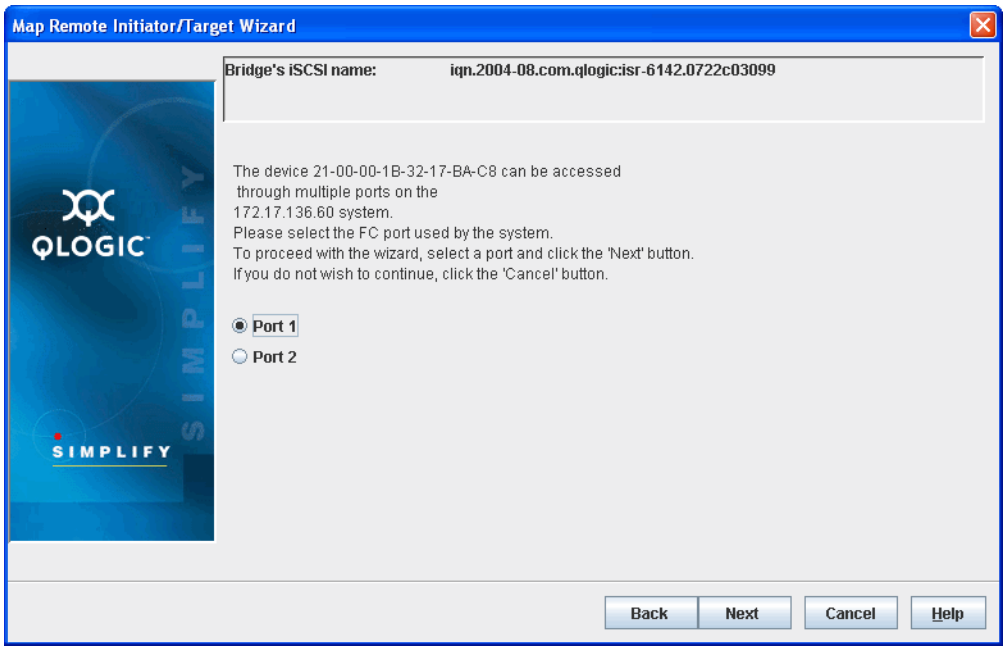

Figure 4-40 Port Selection Dialog Box

4. Select the port the system will use to connect to the device, then click **Next**.

The **Device Mapping Option** dialog box displays SmartWrite mapping options, as shown in Figure 4-41.

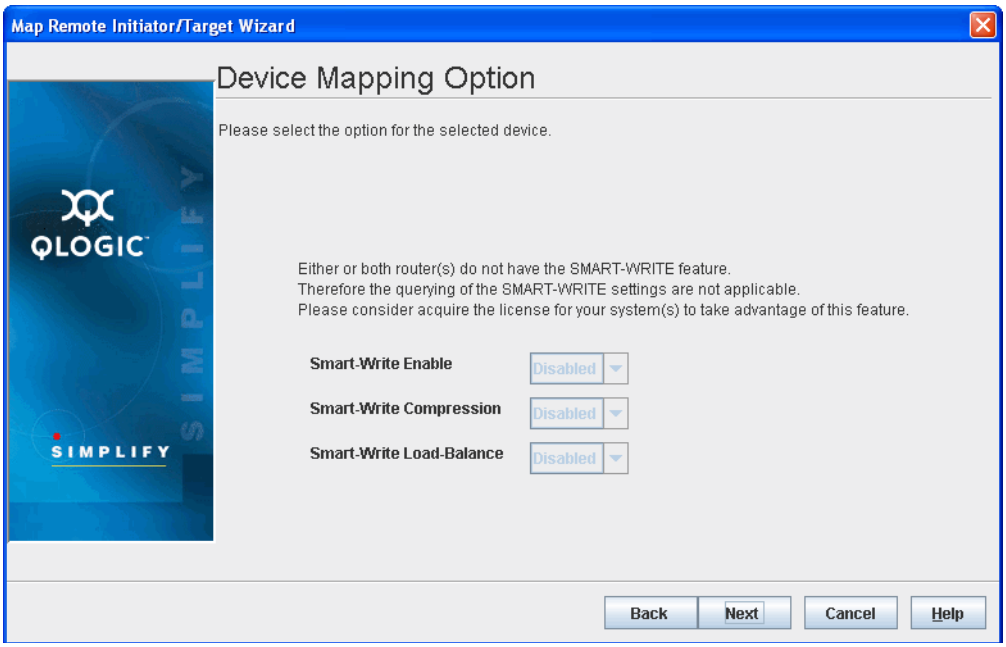

Figure 4-41 Device Mapping Option Dialog Box

5. If your router includes the SmartWrite feature, **Enable** or **Disable** the options as you want.
6. Click **Next.**

The **Confirm Mapping** dialog box displays the mapping and option selections, as shown in Figure 4-42.

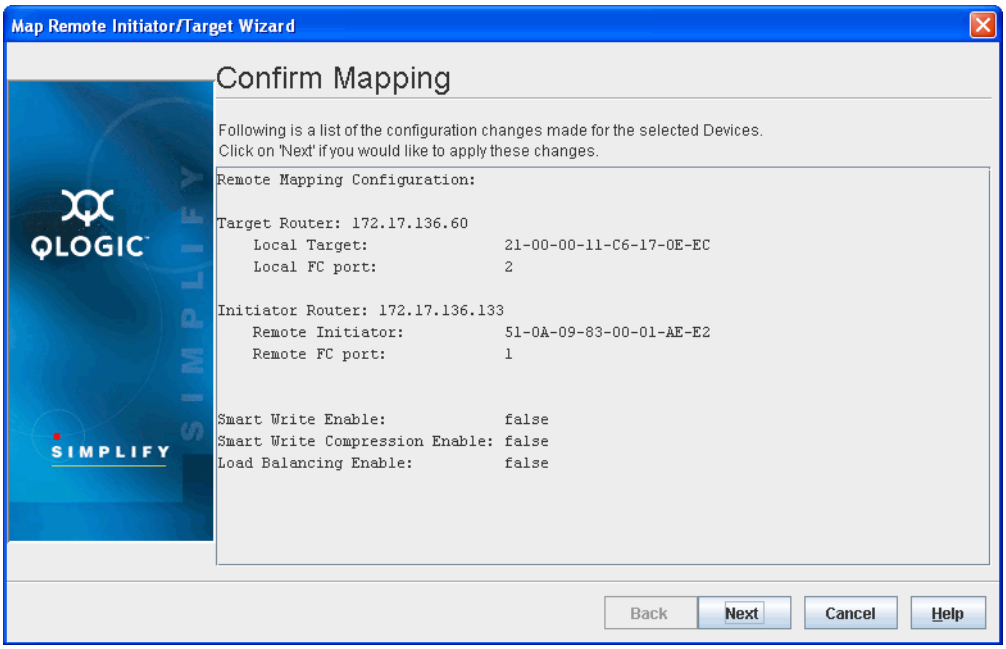

Figure 4-42 Confirm Mapping Dialog Box

7. Review the information and, if correct, click **Next**.

   The **Local Router Admin Password** dialog box displays, as shown in Figure 4-43.

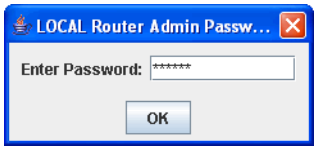

Figure 4-43 Local Password Dialog Box

8. Type the local router admin password (default=config), then click **OK**.

The Remote Mapping Status screen displays a list of newly mapped devices, as shown in Figure 4-44.

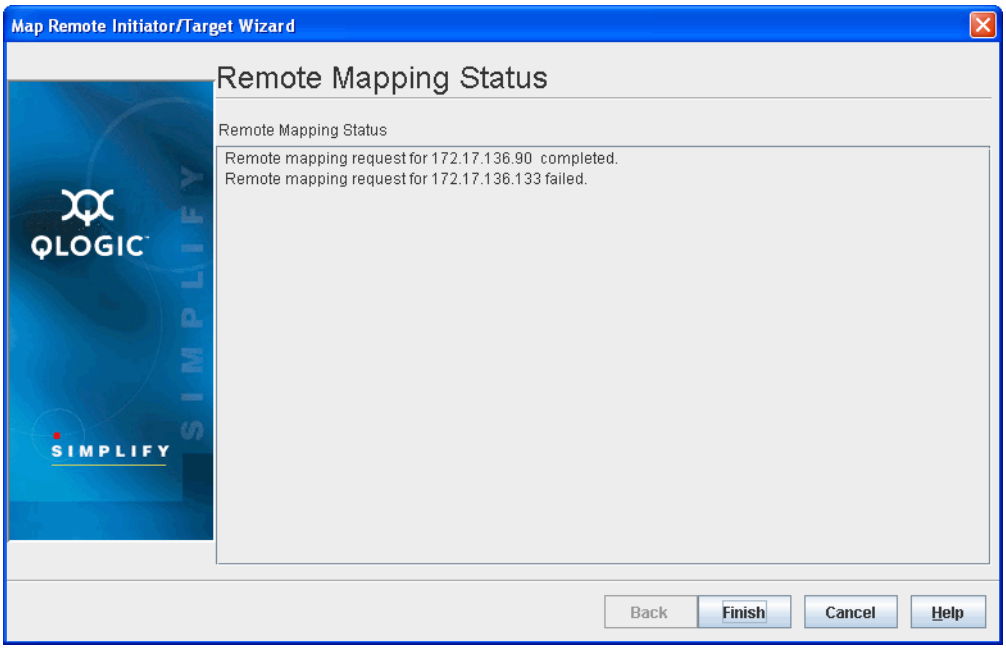

Figure 4-44 Local Router Admin Password Dialog Box

9. Review the status information, then click **Finish**.

   The system prompts you to refresh the display, as shown in Figure 4-45.

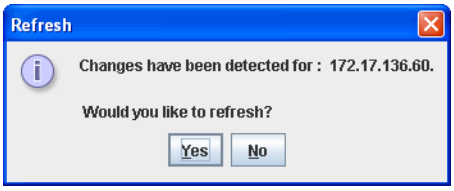

Figure 4-45 Refresh Screen

10. Click **Yes** to refresh the display.

11. View the mapped devices in the router's tree window. Figure 4-46 shows the mapping created in the sample procedures.

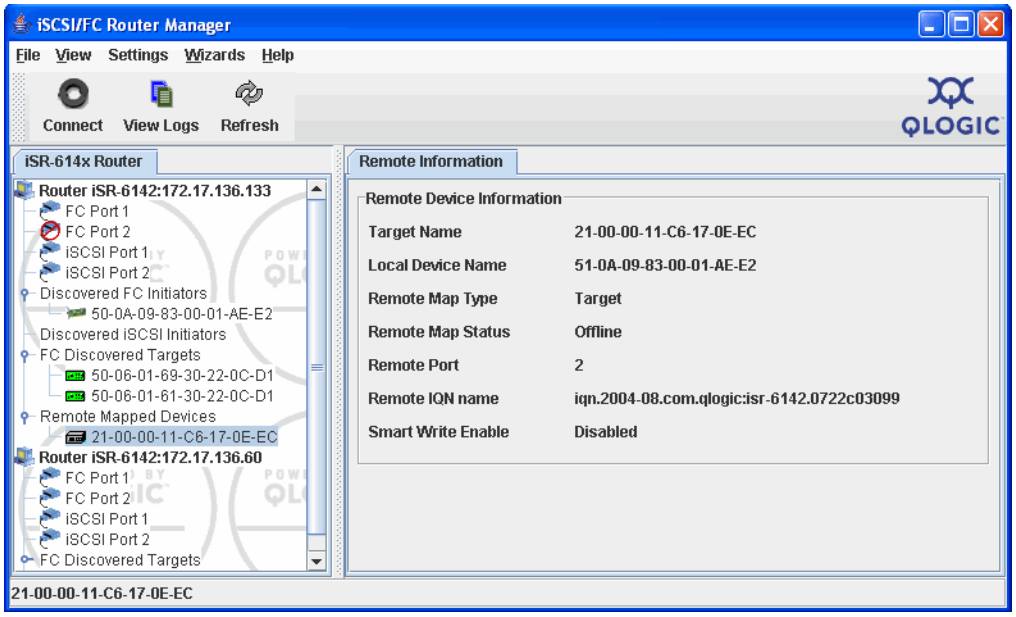

Figure 4-46 Remote Mapped Device

Unmap Remote Initiator/Target Wizard

The Unmap Remote Initiator/Target Wizard provides a set of dialog boxes that walk you through the steps required for removing an initiator-to-target mapping.

You can start this wizard at any time by selecting **Unmap Remote Initiator/Target Wizard** from the Wizards Menu or from the Action Menu.

When the Unmap Remote Initiator/Target Wizard launches, the **Device Selection** dialog box displays a list of remote mapped devices, as shown in Figure 4-47.

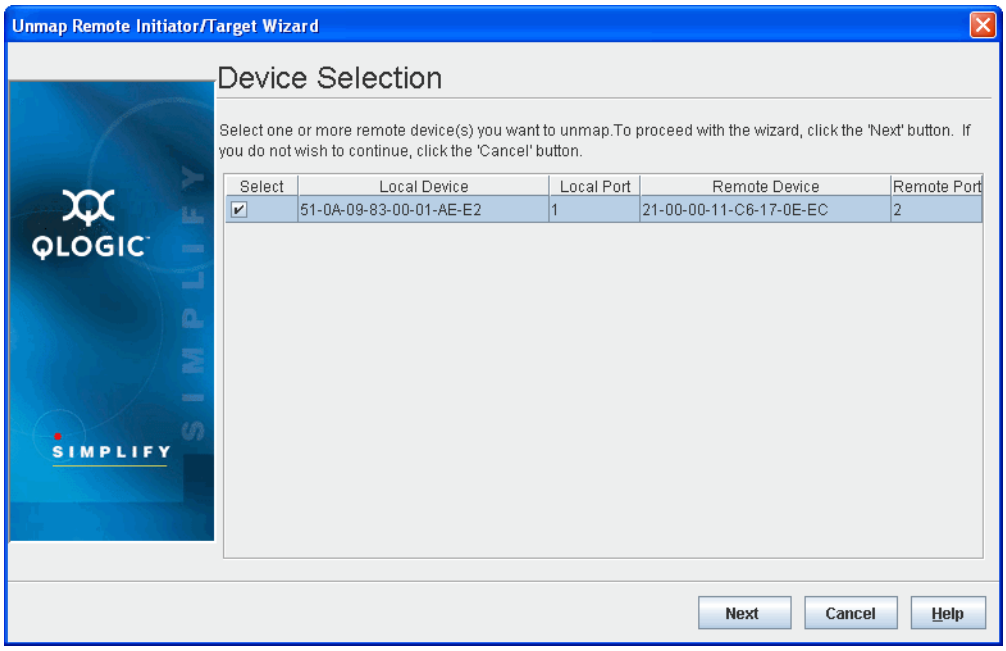

Figure 4-47 Device Selection Dialog Box

To unmap an initiator and target:

1. Select the device to be unmapped, then click **Next**.

The **Local Router's Admin Password** dialog box requests the local router's admin password to continue with the unmap, as shown in Figure 4-48.

Figure 4-48 Local Router Admin Password Dialog Box

2. Type the local router's admin password (default=config), then click **OK**.

   The **Remote Unmap Initiator-Target Status** dialog box displays the status of the unmap operation, as shown in Figure 4-49.

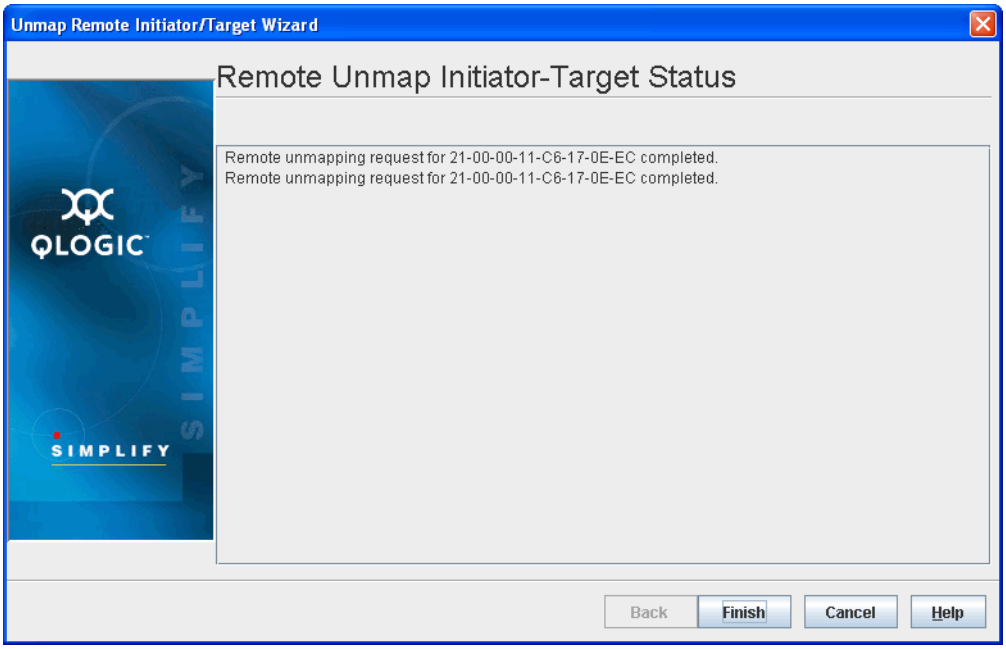

Figure 4-49 Remote Unmap Initiator-Target Status Dialog Box

3. Review the status, then click **Finish**.

Discover iSCSI Target Wizard

The Discover iSCSI Target Wizard provides a set of dialog boxes that walk you through the steps required for discovering an iSCSI target.

You can start this wizard at any time by selecting **Discover iSCSI Target** from the Wizards Menu or from the Action Menu.

When the Discover iSCSI Target Wizard launches, the first window requests you to enter data: an IP address for the iSCSI target, the target's TCP port number (default is 3260) and the router's GE port to be used for the discovery, as shown in Figure 4-50.

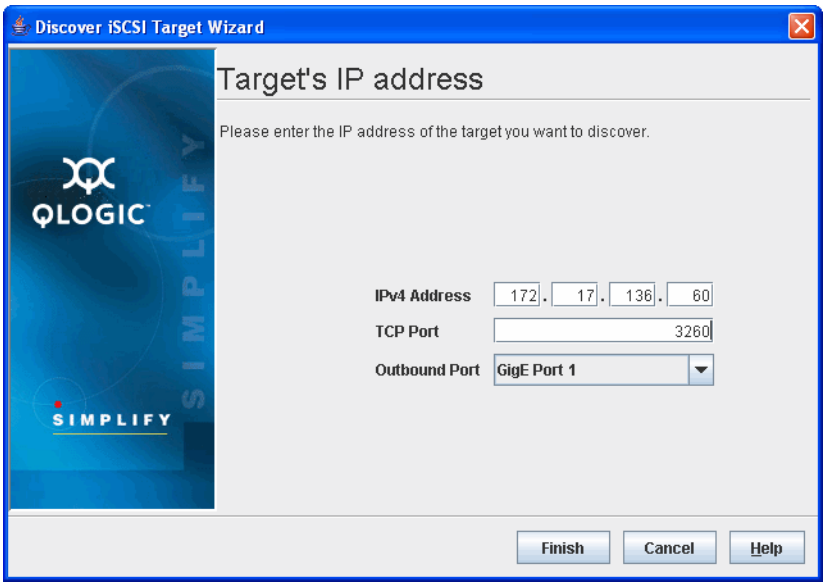

Figure 4-50 Discover iSCSI Target Wizard—IP Address Dialog Box

To discover an iSCSI target:

1. Enter the IP address.
2. Select the GE port from the **Outbound Port** drop-down list.
3. Click **Finish** to initiate the discovery operation.

The **Security Check** dialog box requests the administrator password, as shown in Figure 4-51.

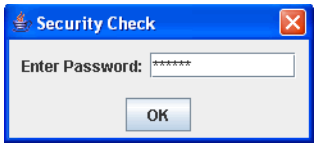

Figure 4-51 Discover iSCSI Target Wizard—Security Check Dialog Box

4. Type the appropriate password, then click **OK** to confirm the discovery of the iSCSI target.

   If the wizard detected iSCSI targets, the **Refresh** dialog box signifies the discovery of the iSCSI target, as shown in Figure 4-52. This dialog box may take a few seconds before appearing.

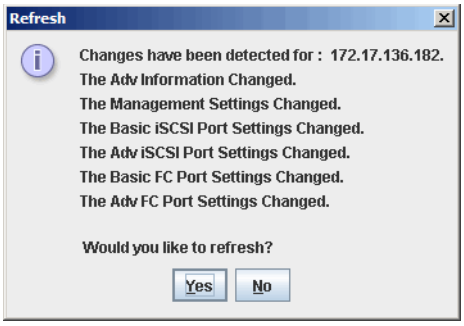
Refresh
Changes have been detected for : 172.17.136.182.
The Adv Information Changed.
The Management Settings Changed.
The Basic iSCSI Port Settings Changed.
The Adv iSCSI Port Settings Changed.
The Basic FC Port Settings Changed.
The Adv FC Port Settings Changed.
Would you like to refresh?
Yes
No

Figure 4-52 Discover iSCSI Target Wizard—Refresh Dialog Box

5. Click **Yes** to refresh system tree with the discovered iSCSI target, or click **No** to skip the refresh.

After the refresh is complete, you can see the Discovered iSCSI Target in the system tree, as shown in Figure 4-53.

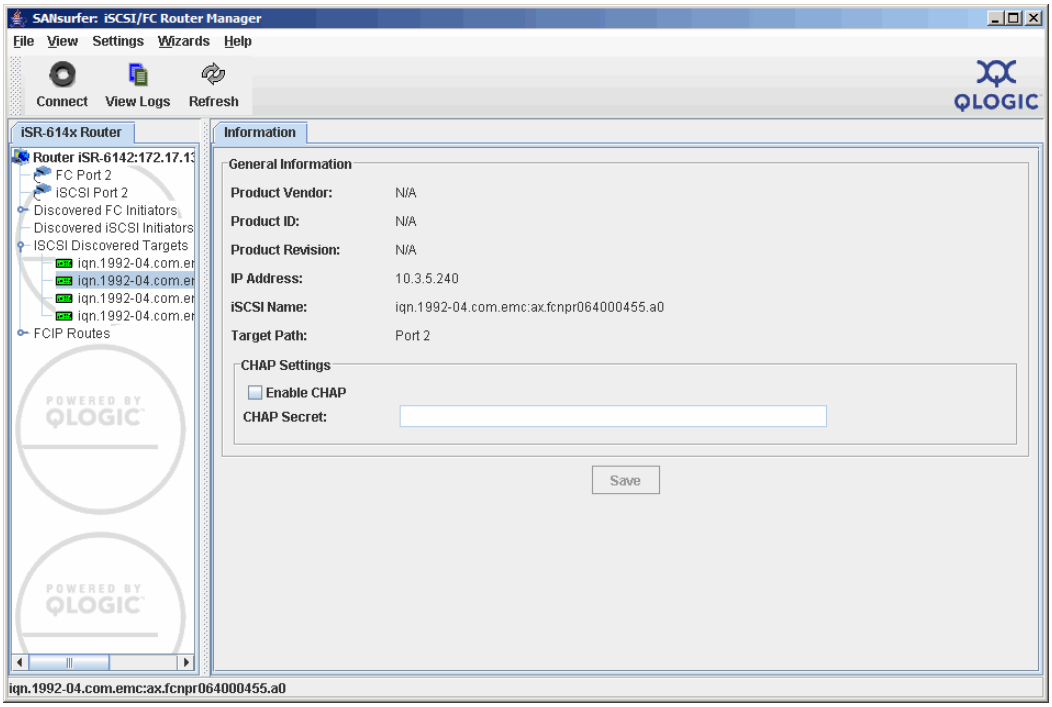

Figure 4-53 iSCSI Discovered Targets

FCIP Route Add Wizard

The FCIP Route Add Wizard provides a set of dialog boxes that walk you through the steps required for adding an FCIP route.

You can start this wizard at any time by selecting **FCIP Route Add** from the Wizards Menu or from the Action Menu.

When the FCIP Route Add Wizard launches, it displays a warning message, letting you know the operation may drop the connection to the selected GE and FC ports. If the router uses the selected ports in FC or iSCSI mappings, it will lose connectivity to them. Using this wizard will also momentarily disrupt connectivity on the GE port not selected for the FCIP route.

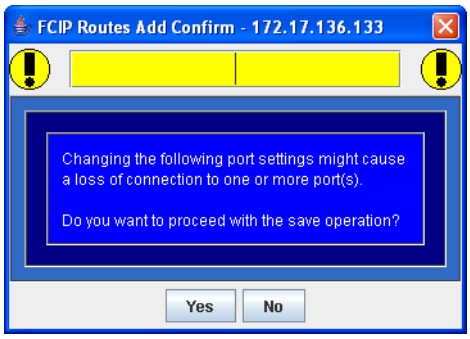
FCIP Routes Add Confirm - 172.17.136.133
Changing the following port settings might cause a loss of connection to one or more port(s).
Do you want to proceed with the save operation?
Yes
No

Figure 4-54 FCIP Route Add Wizard—Warning Dialog Box

To add an FCIP route:

1. Read the warning. If you want to proceed, click **Yes** and continue with step 2. Otherwise, click **No** to cancel the wizard.

The **FC and GigE Port Selection** dialog box prompts you to select an FC-GigE port pair, as shown in Figure 4-55.

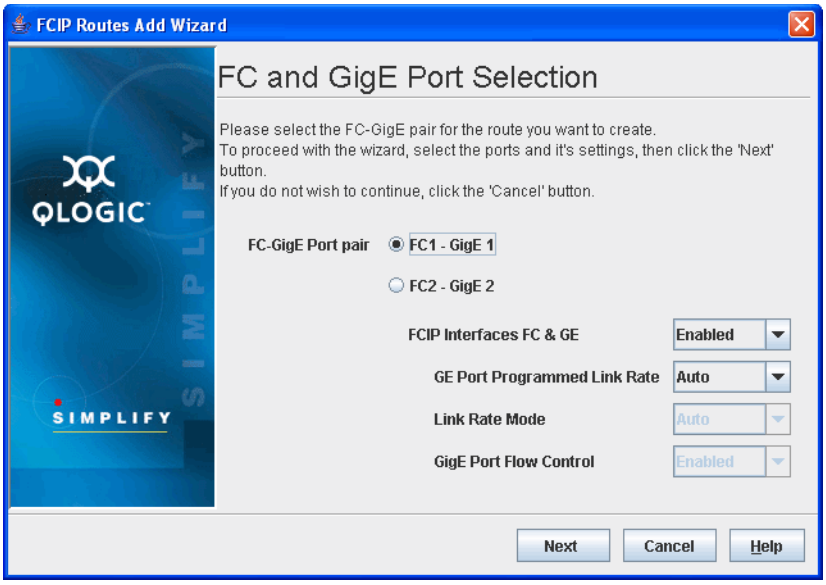
FCIP Routes Add Wizard
FC and GigE Port Selection
Please select the FC-GigE pair for the route you want to create.
To proceed with the wizard, select the ports and it's settings, then click the 'Next' button.
If you do not wish to continue, click the 'Cancel' button.
FC-GigE Port pair
FC1 - GigE 1
FC2 - GigE 2
FCIP Interfaces FC & GE
Enabled
GE Port Programmed Link Rate
Auto
Link Rate Mode
Auto
GigE Port Flow Control
Enabled
Next
Cancel
Help
QLOGIC
SIMPLIFY

Figure 4-55 FCIP Route Add Wizard—Port Selection Dialog Box

2. Select the FC-GigE Port pair. The corresponding parameter options become available.
3. If desired, configure the following port route/parameters:
   - **FCIP Interfaces FC & GE** – Provides a drop-down box you can use to enable or disable the FCIP route. Disabling the route places the FC and GE ports in a down state. It still retains all route configuration parameters.
   - **GigE Port Programmed Link Rate** – Provides a drop-down box you can use select one of four options for the GigE link rate: **Auto**, **10**, **100**, or **1000**. The default link rate is **Auto**.
   - **Link Rate Mode** – Provides a drop-down box you can use select one of three options for the link rate mode: **Auto**, **Half Duplex**, or **Full Duplex**. This dialog box is available only when the GigE link rate is set to something other than **Auto**.
   - **GigE Port Flow Control** – Provides a drop-down box you can use to enable or disable GigE port flow control. The default is enabled. This dialog box is available only when the GigE link rate is set to something other than **Auto**.
4. After selecting a port pair and setting GE port parameters, click **Next** to continue or click **Cancel** to quit the wizard.

The **Local and Remote IP Address** dialog box requests entry of IP addresses (see Figure 4-56).

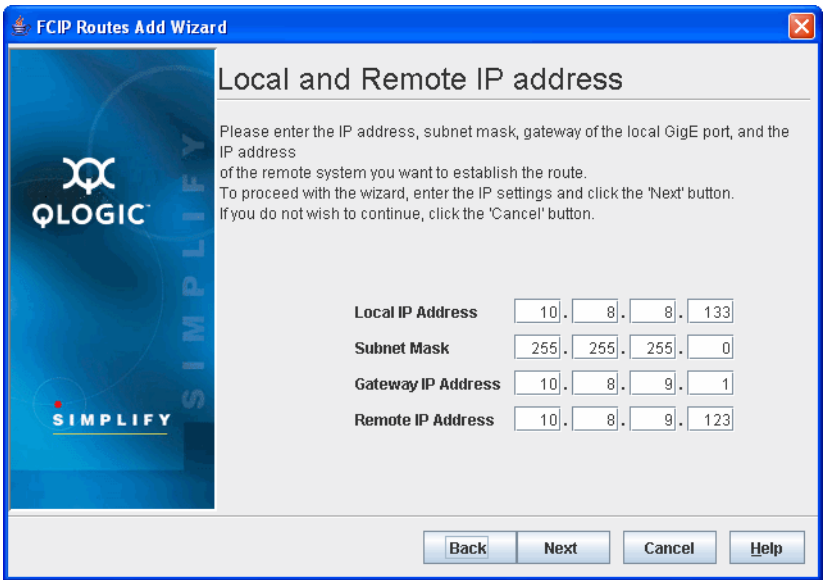
FCIP Routes Add Wizard
Local and Remote IP address
Please enter the IP address, subnet mask, gateway of the local GigE port, and the IP address
of the remote system you want to establish the route.
To proceed with the wizard, enter the IP settings and click the 'Next' button.
If you do not wish to continue, click the 'Cancel' button.
QLOGIC
SIMPLIFY
Local IP Address 10 . 8 . 8 . 133
Subnet Mask 255 . 255 . 255 . 0
Gateway IP Address 10 . 8 . 9 . 1
Remote IP Address 10 . 8 . 9 . 123
Back
Next
Cancel
Help

Figure 4-56 FCIP Route Add Wizard—Local and Remote IP Address Dialog Box

5. Configure any of the following parameters:
   - **Local IP Address** – Enter the IP address the GigE port will use. An uninitialized port has an IP address of all zeros.
   - **Subnet Mask** – Enter the subnet mask the GigE port will use.
   - **Gateway IP Address** – Enter the gateway IP address the GigE port will use.
   - **Remote IP Address** – Enter the IP address of the GigE port the GigE port will use on the remote router.
6. After setting the IP address parameters, click **Next** to continue or click **Cancel** to quit the wizard.

The **TCP/IP Options** dialog box requests entry of TCP/IP parameters, as shown in Figure 4-57.

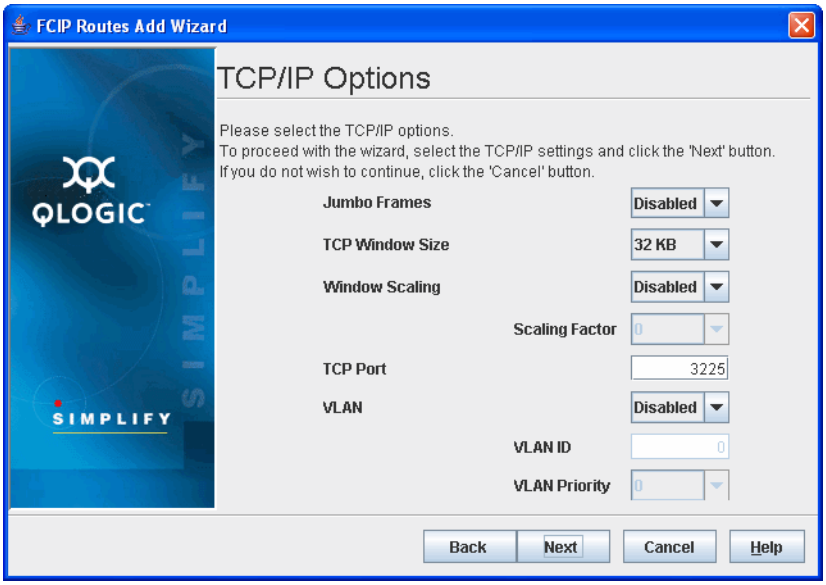

Figure 4-57 FCIP Route Add Wizard—TCP/IP Options Dialog Box

7. Configure any of the following parameters:

   - **Jumbo Frames** – Provides a drop-down box you can use to enable or disable Jumbo IP frames. When disabled the MTU is 1500 bytes. When enabled the MTU is 9000 bytes.

     NOTE:

     An MTU size greater than 1500 should only be used when the router is connected to a 1000 Mbps Ethernet network.

   - **TCP Window Size** – Provides a drop-down box you can use select one of three options for TCP window size: **8192**, **16384**, or **32768** bytes. The default is **32768**.
   - **Window Scaling** – Provides a drop-down box you can use to enable or disable window scaling. The default is disabled.
   - **Window Scaling Factor** – Provides a drop-down box you can use select one of six options for TCP window scaling, any number between **0**–**5**.
   - **VLAN Enabled** – Provides a drop-down box you can use to enable or disable VLAN support. The default is disabled.

- **VLAN ID** – Provides a text field you can use to enter the VLAN ID. This option is available only when VLAN is enabled. The VLAN ID must be the same on both routers participating in the FCIP route (that is, local and remote routers must be using same VLAN ID) and the Ethernet switches.
- **VLAN Priority** – Provides a drop-down box that contains eight options for the VLAN priority: any number between **0**–**7**. This dialog box is available only when VLAN is enabled.

8. After setting the TCP/IP parameters, click **Next** to continue or click **Cancel** to quit the wizard.

   The **FCIP Options** dialog box requests entry of FCIP parameters, as shown in Figure 4-58.

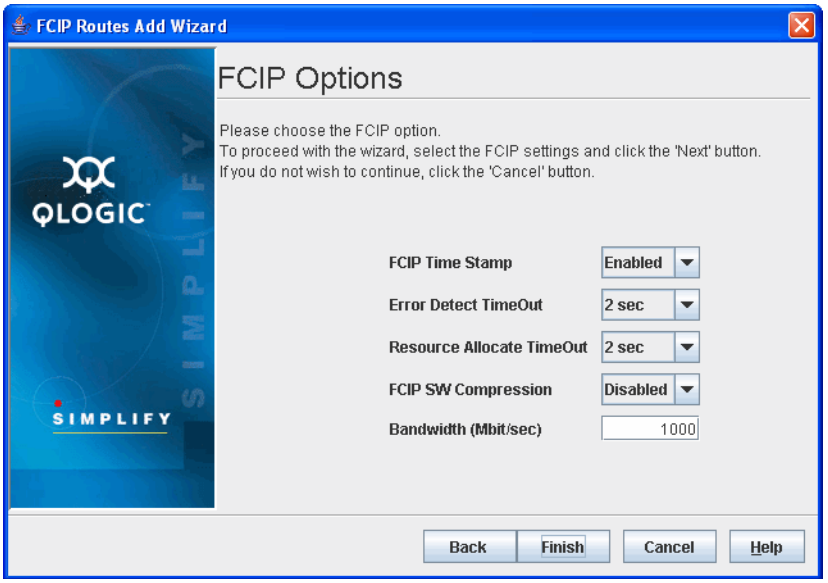

Figure 4-58 FCIP Route Add Wizard—FCIP Options Dialog Box

9. Configure any of the following parameters:
   - **FCIP Timestamp** – Provides a drop-down box you can use to enable or disable FCIP timestamps. The default is enabled.
   - **Error Detect Timeout** – Provides a drop-down box you can use to select one of five options for the error detect timeout: any number between **1** to **5** seconds. The default is one second.
   - **Resource Allocate Timeout** – Provides a drop-down box you can use to select one of five options for the resource allocate timeout: any number between **1** to **5** seconds. The default is one second.

- **FCIP SW Compression** – Provides a drop-down box you can use to enable or disable FCIP compression. The default is disabled.
- **Bandwidth (Mbit/sec)** – Provides a text field in which you can enter the maximum bandwidth (in megabits per second) used by the GigE port during transmits. The range of values supported is `1` to `1000` megabits per second. This setting allows you to limit the bandwidth used by the FCIP route so as to not consume all the available link bandwidth. For example, if the slowest link in the WAN being used is a DS-3 link, the maximum available bandwidth is `45` megabits per second. To limit the FCIP route to 33% of the overall link bandwidth set the bandwidth to `15` megabits per second.

10. After setting the FCIP parameters, click **Next** to continue or click **Cancel** to quit the wizard.

    The **Security Check** dialog box requests the administrator password, as shown in Figure 4-59.

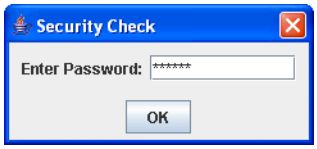

Figure 4-59 FCIP Route Add Wizard—Security Check Dialog Box

11. Type the appropriate password, then click **OK** to confirm adding the FCIP route.

    The **Add FCIP Route Complete** dialog box lets you know when the configuration is complete, as shown in Figure 4-60.

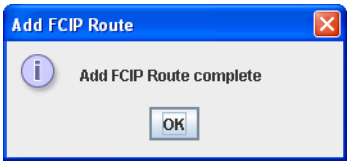

Figure 4-60 FCIP Route Add Wizard—Completed Dialog Box

NOTE:

This dialog box may take a few seconds before appearing.

12. Click **OK** to exit the dialog box.

FCIP Route Remove Wizard

The FCIP Route Remove Wizard provides a set of dialog boxes that walk you through the steps required for removing an FCIP route.

You can start this wizard at any time by selecting **FCIP Route Remove** from the Wizards Menu or from the Action Menu.

When the FCIP Route Remove Wizard launches, it displays a warning message, letting you know the operation may drop the connection to the selected GE and FC ports. If the router uses the selected ports in FC or iSCSI mappings, it will lose connectivity to them. Using this wizard will also momentarily disrupt connectivity on the GE port not selected for the FCIP route.

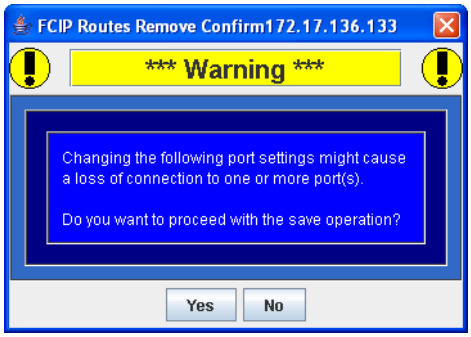
FCIP Routes Remove Confirm172.17.136.133
*** Warning ***
Changing the following port settings might cause a loss of connection to one or more port(s).
Do you want to proceed with the save operation?
Yes
No

Figure 4-61 FCIP Route Remove Wizard—Warning Dialog Box

To remove an FCIP route:

1. Read the warning. If you want to proceed, click **Yes** and continue with step 2. Otherwise, click **No** to cancel the wizard.

The FCIP Remove dialog box displays a list of existing FCIP routes, as shown in Figure 4-62.

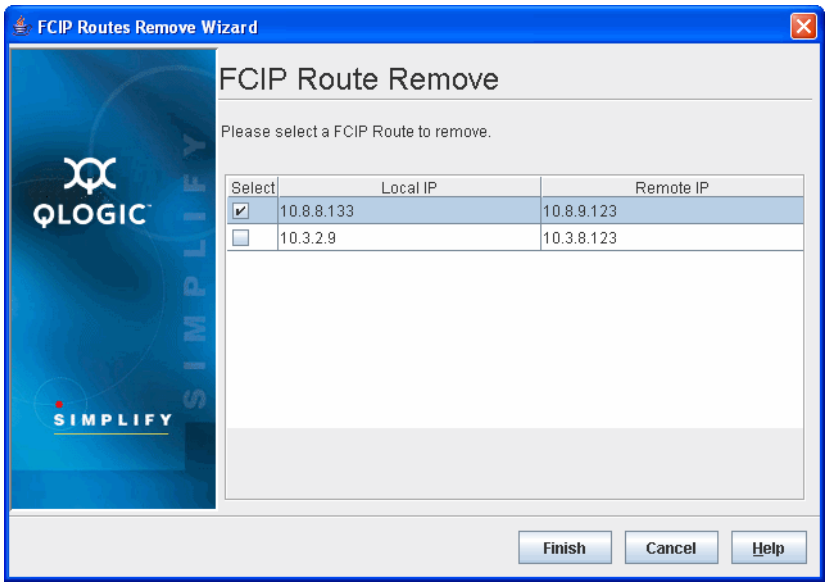

Figure 4-62 FCIP Route Remove Wizard—Route Selection Dialog Box

2. Select the FCIP route you want to remove, then click **Finish**.

   The **Security Check** dialog box requests the administrator password, as shown in Figure 4-63.

Figure 4-63 FCIP Route Remove Wizard—Security Check Dialog Box

3. Type the appropriate password, then click **OK** to confirm the removal of the FCIP route.

The **Add FCIP Route Complete** dialog box lets you know when the configuration is complete, as shown in Figure 4-64.

Figure 4-64 FCIP Route Remove Wizard—Completed Dialog Box

NOTE:

This dialog box may take a few seconds before appearing.

4. Click **OK** to exit the dialog box.

Notes

5 Configuring CHAP

This chapter describes CHAP and provides the procedures for configuring CHAP using the SANsurfer Router Manager.

For procedures, see the following sections:

- "Discovery Session—Bi-directional CHAP" on page 5-2
- "Discovery Session—Uni-directional CHAP" on page 5-3
- "Normal Session—Bi-directional CHAP" on page 5-3
- "Normal Session—Uni-directional CHAP" on page 5-4

CHAP Definition

In challenge handshake authentication protocol (CHAP), the authentication agent sends the client program a random value that is used only once and an ID value. Both the sender and peer share a predefined secret. The peer concatenates the random value, the ID, and the secret, and calculates a one-way hash using MD5 (Message-Digest algorithm 5). It sends the hash value to the authenticator, which in turn builds that same string on its side, calculates the MD5 checksum, and compares the result with the value received from the peer. If the values match, the peer is authenticated.

By transmitting only the hash, the secret cannot be reverse-engineered. The ID value is increased with each CHAP dialogue to protect against replay attacks.

Discovery Session—Bi-directional CHAP

To configure a bi-directional CHAP during a discovery session:

1. On the bridge, enable CHAP for the iSCSI port.
2. Select the port in the left column.
3. Click **Advanced Configuration**.
4. Select **Enable Chap**.
5. Type a secret in **Chap secret** (for example, *secret_port*).
6. Check to see if the initiator exists on the discovered iSCSI initiators list:
   - If the initiator *is not* part of the discovered iSCSI initiators list, then go to the wizard menu and select **Add Initiator Wizard**.
   - If the initiator is part of the discovered list, then go to Step 10.
7. Type the IQN name string.
8. Select **Enable CHAP**.
9. Create a CHAP secret (for example, *secret_initiator*).
10. Go to the MS Initiator and perform the following steps:
    a. Click **General**.
    b. Click **Secret** (in the middle of the screen).
    c. If this is the first time you are setting secrets, reset all secrets.
    d. Type the CHAP secret (*secret_port*) that you created in Step 5.
11. Click **Discovery**.
12. Click **Add**.
13. Enter the address of the iSCSI port of the bridge.
14. Click **Advanced**.
15. Select **Chap Login Information**.
16. Type the secret (*secret_initiator*) that you created in Step 9 into **Target Secret**.
17. Select **Mutual Authentication**.
18. Click **OK**.
19. Click **OK**. The initiator completes discovery.

Discovery Session—Uni-directional CHAP

To program a single-direction CHAP during a discovery session:

1. Do not enable CHAP on the iSCSI port.
2. Check to see if the initiator exists on the discovered iSCSI initiators list:
   - If the initiator *is not* part of the discovered iSCSI initiators list, then go to the wizard menu and select **Add Initiator Wizard**.
   - If the initiator is part of the discovered list, then go to Step 6.
3. Type the IQN name string.
4. Select **Enable Chap**.
5. Create a CHAP secret (for example, *secret_initiator*).
6. Go to the MS Initiator and perform the following steps:
   a. Click **Discovery**.
   b. Click **Add**.
   c. Enter the address of the iSCSI port of the bridge.
   d. Click **Advanced**.
   e. Click **Chap Login Information**.
   f. Type the secret (*secret_initiator*) you created in Step 5 into **Target Secret**.
7. Click **OK**.
8. Click **OK**. The initiator completes discovery.

Normal Session—Bi-directional CHAP

To program bi-directional CHAP during a normal session:

1. On the bridge, enable CHAP for the iSCSI presented target.
2. Select the presented target on the left column of the SANsurfer Router Manager.
3. Click **Information**.
4. Select **Enable Chap**.
5. Type a secret in the **Chap secret** dialog box (for example, *secret_target*).

6. Check to see if the initiator exists on the discovered iSCSI initiators list:
   - If the initiator *is not* part of the discovered iSCSI initiators list, then go to the wizard menu and select **Add Initiator Wizard**.
   - If the initiator is part of the discovered list, then go to Step 10.
7. Fill in the IQN name string.
8. Select **Enable Chap**.
9. Create a CHAP secret (for example, *secret_initiator*).
10. Go to the MS Initiator and perform the following steps:
    a. Click **General**.
    b. Click **Secret** (in the middle of the screen).
    c. If this is the first time you are setting secrets, reset all the secrets.
    d. Type the secret (*secret_target*) that you created in Step 5.
11. Click **Targets**.
12. Select the target you want to login to.
13. Click **Log On**.
14. Click **Advanced**.
15. Select **Chap Login Information**.
16. Type the secret (*secret_initiator*) that you created in Step 9 into **Target Secret**.
17. Select **Mutual Authentication**.
18. Click **OK**.
19. Click **OK**. The initiator completes normal login.

Normal Session—Uni-directional CHAP

To program single-direction CHAP during a normal session:

1. Do not enable CHAP on the iSCSI presented target.
2. Check to see if the initiator exists on the discovered iSCSI initiators list:
   - If the initiator *is not* part of the discovered iSCSI initiators list, then go to the wizard menu and select **Add Initiator Wizard**.
   - If the initiator is part of the discovered list, then go too Step 6.
3. Fill in the IQN name string.
4. Select **Enable Chap**.

5. Create a CHAP secret (for example, *secret_initiator*).
6. Go to the MS Initiator and perform the following steps:
   a. Click **Targets**.
   b. Select the target you want to login to.
   c. Click **Log On**.
   d. Click **Advanced**.
   e. Click **Chap Login Information**.
   f. Type the secret (*secret_initiator*) you created in Step 5 into **Target Secret**,
   g. Click **OK**.
7. Click **OK**. The initiator completes normal login.

Notes

A Log Messages

This appendix provides reference material on messages logged to a file.

You can view these message logs from the SANsurfer Router Manager using any of these methods:

- Select **View Logs** from the View menu.
- Click the **View Logs** tool bar icon.
- Right-click anywhere within the router's node in the system tree window and select **View Logs** from the action menu.

Log Data

The message log is persistent, maintained across router power cycles and reboots. The three log message categories are:

- Informational
- Error (see page A-10)
- Fatal (see page A-10)

The following sections describe the log message categories.

Informational Log Messages

The following sections list and describe the informational log messages by reporting module:

- "Application Modules" on page A-2
- "iSCSI Driver" on page A-4
- "Fibre Channel Driver" on page A-5
- "User Modules" on page A-6
- "FCIP" on page A-8
- "TOE Driver" on page A-9
- "System" on page A-9

Application Modules

The application modules generate the informational log messages listed in Table A-1 and described following the table.

Table A-1. Application Modules—Informational Log Messages

ID	Log Message	No.
53254	System (router) Booting up	6
53357	QLBA_ProcessTpb: De-compression failed. Disabling compression temporarily	109
54274	QLFC_Login: Origin 0x%x, VP Index 0x%x, Id 0x%x	1026
54275	QLFC_Login: Port ID %.2x%.2x%.2x	1027
54276	QLFC_Login: Node Name %.2x%.2x%.2x%.2x%.2x%.2x%.2x%.2x	1028
54277	QLFC_Login: Port Name %.2x%.2x%.2x%.2x%.2x%.2x%.2x%.2x	1029
54306	QLFC_Logout: Origin 0x%x, VP Index 0x%x, Id 0x%x	1058
54307	QLFC_Logout: Port ID %.2x%.2x%.2x	1059
54308	QLFC_Logout: Node Name %.2x%.2x%.2x%.2x%.2x%.2x%.2x%.2x	1060
54309	QLFC_Logout: Port Name %.2x%.2x%.2x%.2x%.2x%.2x%.2x%.2x	1061
54359	QLFC_HandleTeb: FC Login. VP 0x%x	1111
54368	QLFC_CreateVirtualInitiatorObject: Maximum host (%d) limit reached.	1120
54938	QLIS_HandleTeb: UTM_EC_OPEN_CONNECTION	1690
54939	QLIS_HandleTeb: UTM_EC_CLOSE_CONNECTION or UTM_EC_CONNECTION_CLOSED	1691
54940	QLIS_HandleTeb: UTM_EC_CONNECTION_OPENED	1692
54941	QLIS_HandleTeb:iSNS Server Open Connection succeeded	1693
54943	QLIS_HandleTeb: UTM_EC_ISNS_SCN	1695
54945	QLIS_HandleTeb: UTM_EC_ISNS_CLIENT_DISCOVERED	1697
54947	QLIS_HandleTeb: UTM_EC_CLOSE_CONNECTION	1699
54948	QLIS_HandleTeb: UTM_EC_CONNECTION_CLOSED	1700

Table A-1. Application Modules—Informational Log Messages (Continued)

ID	Log Message	No.
54963	QLIS_SetDdbEntryContinue:[%d:%d] Remote system connection established	1715
54986	QLIS_HandleSessionTimer: Re-enabling compression	1738
55299	QLSC_CollectBUVUIO: Freeing dead TRB: State 0x%02X, AbortReason %d, Flags 0x%02X	2051

6	Router is booting up.
109	De-compression failed and will be temporarily disabled.
1026	FC login occurred, origin xx (1 = HBA, 2 = target, 3 = initiator), VP (virtual port) xx, ID (loop ID) xx.
1027	FC login occurred with port ID xx.xx.xx.
1028	FC login occurred with WWNN xx.xx.xx.xx.xx.xx.xx.xx.
1029	FC login occurred with WWPN xx.xx.xx.xx.xx.xx.xx.xx.
1058	FC logout occurred, origin xx (1 = HBA, 2 = target, 3 = initiator), VP (virtual port) xx, ID (loop ID) x.
1059	FC logout occurred with port ID xx.xx.xx.
1060	FC logout occurred with WWNN xx.xx.xx.xx.xx.xx.xx.xx.
1061	FC logout occurred with WWPN xx.xx.xx.xx.xx.xx.xx.xx.
1111	FC login event notification, VP (virtual port) xx.
1120	Maximum number of support hosts dd has been reached.
1690	Event notification: iSCSI open connection request.
1691	Event notification: iSCSI close connection request or connection closed.
1692	Event notification: iSCSI connection opened.
1693	Event notification: connection opened with iSNS server.
1695	Event notification: iSNS SCN received.
1697	Event notification: iSNS client discovered.
1699	iSCSI close connection request received.

1700	iSCSI connection closed.
1715	Remote system connection established using DDB d:d.
1738	Re-enabling compression.
2051	TRB freed, State xx, Abort Reason d, Flags xx.

iSCSI Driver

The following informational log messages are common to both iSCSI ports: 1 (GE1) and 2 (GE2). The messages are listed in Table A-2 and described following the table. Log messages beginning with #0 denote iSCSI port 1 (GE1) and log messages beginning with #1 denote iSCSI port 2 (GE2).

Table A-2. iSCSI Driver—Informational Log Messages

ID	Log Message	No.
86343	#%d: QLPortUp: Set link configuration 0x%x	327
86347	#%d: QLDisable: Restart RISC	331
86349	#%d: QLEnable: Restart RISC to update EEPROM	333
86352	#%d: QLPortDown: Set link configuration 0x%x	336
86874	#%d: QLIsrDecodeMailbox: Link up	858

327	iSCSI port enabled, port up.
331	Restart iSCSI processor (RISC).
333	EEPROM updated, restart iSCSI processor (RISC).
336	iSCSI port disabled, port down.
858	Link up reported by iSCSI processor for GE1 or GE 2.

Fibre Channel Driver

The following informational log messages are common to both Fibre Channel ports: 1 (FC1) and 2 (FC2). The messages are listed in Table A-3 and described following the table. Log messages beginning with #0 denote Fibre Channel port 1 (FC1). Log messages beginning with #1 denote Fibre Channel port 2 (FC2).

Table A-3. Fibre Channel Driver—Informational Log Messages

ID	Log Message	No.
118882	#%d: QLIoctlDisable: Reset adapter	98
119088	#%d: QLIsrEventHandler: LIP occurred (%x): mailbox1 = %x	304
119089	#%d: QLIsrEventHandler: LIP reset occurred (%x): mailbox1 = %x	305
119090	#%d: QLIsrEventHandler: Link up (%x) mailbox1 = %x	306
119092	#%d: QLIsrEventHandler: Link mode up (%x): RunTimeMode=%x	308
119093	#%d: QLIsrEventHandler: RSCN update (%x) rscnInfo: %x	309
119097	#%d: QLIsrEventHandler: Port update (%x) mb1-3 %x %x %x	313
119552	#%d: QLFcipIsrEventHandler: Link up (%x) mailbox1 = %x	768
119553	#%d: QLFcipIsrEventHandler: Link down (%x)	769
119554	#%d: QLFcipIsrEventHandler: Link mode up (%x)	770

98	Request to reset the FC processor (adapter) received from IOCTL interface.
304	Fibre Channel loop initialization procedure (LIP) occurred. The LIP type is reported, as is the contents of the FC processor's mailbox 1 register.
305	Fibre Channel LIP reset occurred. The LIP reset type is reported, as is the contents of the FC processor's mailbox 1 register.
306	Fibre Channel link up occurred. Event status is reported, as is the contents of the FC processor's mailbox 1 register.
308	Fibre Channel link up occurred. Event status is reported, as is the RunTimeMode (0 = loop, 1 = point-to-point).
309	A RSCN was received. Event status is reported, as is the RSCN information.
313	Fibre Channel port update. Event status is reported, as is the contents of the FC processor's mailbox 1, 2, and 3 registers.

768	FCIP - Fibre Channel link up occurred. Event status is reported, as is the contents of the FC processor's mailbox 1 register.
769	FCIP - Fibre Channel link down occurred.
770	FCIP - Fibre Channel link up occurred. Event status is reported, as is the RunTimeMode (0 = loop, 1 = point-to-point).

User Modules

The user modules generate the log messages listed in Table A-4 and described in the following table.

Table A-4. User Modules—Informational Log Messages

ID	Log Message	No.
151842	FW Upgrade performed: new version is: %d.%d.%d.%d	290
151843	REBOOT/SHUTDOWN Command from user. Code=%d	291
151889	#%d: qapisetfcinterfaceparams_1_svc: FC port configuration changed	337
151890	#%d: qapisetiscsiinterfaceparams_1_svc: iSCSI port configuration changed	338
151891	#%d: qapisetisns_1_svc:iSNS configuration changed	339
151892	qapisetntpparams_1_svc: NTP configuration changed	340
151893	#%d: qapisetvlanparams_1_svc: VLAN configuration changed	341
151896	qapisetmgmintfcparams_1_svc:Management port configuration changed	344
151897	qapisetbridgebasicinfo_1_svc:Bridge configuration changed	345
151898	qapimapremote_1_svc: Remotemap added for local device %.2x:%.2x:%.2x:%.2x:%.2x:%.2x:%.2x:%.2x	346
151899	qapimapremote_1_svc: Remotemap added to remote device %.2x:%.2x:%.2x:%.2x:%.2x:%.2x:%.2x:%.2x	347
151900	qapiunmapremote_1_svc: Remotemap removed for local device %.2x:%.2x:%.2x:%.2x:%.2x:%.2x:%.2x:%.2x	348
151901	qapiunmapremote_1_svc: Remotemap removed to remote device %.2x:%.2x:%.2x:%.2x:%.2x:%.2x:%.2x:%.2x	349
151902	qapimaptargettoinitiator_1_svc: Localmap added for initiator %.2x:%.2x:%.2x:%.2x:%.2x:%.2x:%.2x:%.2x	350

Table A-4. User Modules—Informational Log Messages (Continued)

ID	Log Message	No.
151903	qapimaptargettoinitiator_1_svc: Localmap added to target device %.2x:%.2x:%.2x:%.2x:%.2x:%.2x:%.2x:%.2x	351
151904	qapiunmaptargettoinitiator_1_svc: Localmap removed for initiator device %.2x:%.2x:%.2x:%.2x:%.2x:%.2x:%.2x:%.2x	352
151905	qapiunmaptargettoinitiator_1_svc: Localmap removed to target device %.2x:%.2x:%.2x:%.2x:%.2x:%.2x:%.2x:%.2x	353
151906	qapimaptargettoinitiator_1_svc: Localmap added for initiator %s	354
151907	qapiunmaptargettoinitiator_1_svc: Localmap removed for initiator %s	355
151908	GE%d: Port status changed by user to ENABLED.	356
151909	GE%d: Port status changed by user to DISABLED.	357
151910	FC%d: Port status changed by user to ENABLED.	358
151911	FC%d: Port status changed by user to DISABLED.	359
152069	qapisetfcipparams_1_svc: FCIPROUTE %d Added	517
152070	qapisetfcipparams_1_svc: FCIPROUTE %d Modified	518
152071	qapisetfcipparams_1_svc: FCIPROUTE %d Removed	519

290	Performed router firmware upgrade, new version number is d.d.d.d.
291	User performed a router reboot or shutdown.
337	FC port configuration has been modified.
338	iSCSI port configuration has been modified.
339	iSNS configuration has been modified.
340	NTP configuration has been modified.
341	VLAN configuration has been modified.
344	Management Ethernet port configuration has been modified.
345	Router configuration has been modified.
346	Remotemap added for local FC device WWPN xx.xx.xx.xx.xx.xx.xx.xx.
347	Remotemap added for remote FC device WWPN xx.xx.xx.xx.xx.xx.xx.xx.

348	Remotemap removed for local FC device WWPN xx.xx.xx.xx.xx.xx.xx.xx.
349	Remotemap removed for remote FC device WWPN xx.xx.xx.xx.xx.xx.xx.xx.
350	Localmap added for FC initiator WWPN xx.xx.xx.xx.xx.xx.xx.xx.
351	Localmap added to FC target device WWPN xx.xx.xx.xx.xx.xx.xx.xx.
352	Localmap removed for FC initiator.
353	Localmap removed to FC target device.
354	Localmap added for iSCSI initiator "iqn.dddd-dd.ttt.ttt.ttt.....".
355	Localmap removed for iSCSI initiator "iqn.dddd-dd.ttt.ttt.ttt.....".
356	User enabled GE port d.
357	User disabled GE port d.
358	User enabled FC port d.
359	User disabled FC port d.
517	FCIP route #d added.
518	FCIP route #d modified.
519	FCIP route #d removed.

FCIP

The FCIP module generates the informational log messages listed in Table A-5 and described following the table.

Table A-5. FCIP—Informational Log Messages

ID	Log Message	No.
184524	qlFcip_Linkchange#%d: GigE Link Down	204
184525	qlFcip_Linkchange#%d: GigE Link Up	205

204	FCIP Route GigE link d (1 or 2) is down.
205	FCIP Route GigE link d (1 or 2) is up.

TOE Driver

The TOE driver generates the informational log messages listed in Table A-6 and described following the table.

Table A-6. TOE—Informational Log Messages

ID	Log Message	No.
217350	QL3022:eth%x: Interface is down	262

262 The GigE interface d (0 or 1) used for an FCIP route is down.

System

The system modules generate the informational log messages listed in Table A-7 and described following the table.

Table A-7. System—Informational Log Messages

ID	Log Message	No.
249862	“Temperature is back to normal range %d\n"	6

6 The router temperature has returned to the normal operating range and is d (C).

Error Log Messages

The following sections list and describe the error log messages by reporting module:

- "Application Modules" on page A-10
- "iSCSI Driver" on page A-18
- "Fibre Channel Driver" on page A-20
- "User Modules" on page A-22
- "System" on page A-25

Application Modules

The application modules generate the error log messages listed in Table A-8 and described following the table.

Table A-8. Application Module—Error Log Messages

ID	Log Message	No.
40967	QLBA_NullDoorbell: driver unloaded, port disabled	7
40996	QLBA_ProcessTrb: Processing unsupported ordered tag command	36
41004	QLBA_ProcessTrb: Processing unsupported head of queue tag command	44
41058	QLBA_CreateTargetDeviceObject: Too many devices	98
41060	QLBA_CreateTargetNodeObject: Too many devices	100
41067	QLBA_CreateLunObject: LunObject memory unavailable	107
41077	QLBA_CreateInitiatorObject: Too many initiators	117
41096	QLBA_DisplayTargetOperationStatus: PCI Error, Status 0x%.2x	136
41106	QLBA_DisplayInitiatorOperationStatus: DMA Error, Status 0x%.2x	146
41107	QLBA_DisplayInitiatorOperationStatus: Transport Error, Status 0x%.2x	147
41111	QLBA_DisplayInitiatorOperationStatus: Data Overrun, Status 0x%.2x	151
41234	QLIS_LoginPduContinue: Operation failed. Initiator 0x%x, TPB status 0x%x	274
41238	QLKV_ValidateLoginTransitCsgNsgVersion failed (status 0x%x)	278

Table A-8. Application Module—Error Log Messages (Continued)

ID	Log Message	No.
41257	QLIS_LoginPduContinue: Invalid initiator name. Initiator:	297
41265	QLIS_LoginPduContinue: Target not configured for Portal	305
41267	QLIS_LoginPduContinue: Target not found. Target name:	307
41268	QLIS_LoginPduContinue: Missing target name	308
41270	QLIS_LoginPduContinue: TSIH is 0 but InitiatorName key/value not provided	310
41272	QLIS_LoginPduContinue: CONN_STATE_IN_LOGIN, Unknown InitTaskTag	312
41283	QLIS_LoginPduContinue: TSIH 0x%x out of range	323
41284	QLIS_LoginPduContinue: Session does not exist, invalid TSIH 0x%x	324
41353	QLIS_LoginPduContinue CHAP Validation Failure	393
41354	QLIS_LoginPduContinue Unexpected CHAP key detected	394
41508	QLBI_SetPortInfo: QLUT_AllocatePortalObject failed (PortType 0x%x, PortId 0x%x)	548
41626	QLBI_GetLunInfo: INQUIRY failed, TPB status 0x%x	666
41629	QLBI_GetLunInfo: QLBI_PassthruCommand failed for INQUIRY (page code 0x83)	669
41635	QLBI_GetLunInfo: QLBI_PassthruCommand failed for READ CAPACITY	675
41636	QLBI_GetLunInfo: READ CAPACITY failed, TPB status 0x%x	676
41696	QLBI_PassthruCommandCompletion: Passthru command aborted	736
41700	QLBI_Passthru: Invalid CDB length %d bytes	740
41701	QLBI_Passthru: Invalid data length %d bytes	741
41717	QLBI_PassthruCommand: command interrupted or timed out	757
41750	QLBI_Ioctl: ERROR: Operation (0x%x) not supported in this mode	790
41768	QLBI_GetLunList: REPORT LUNS command failed	808
41769	QLBI_GetLunList: REPORT LUNS command failed with CHECK CONDITION, SCSI STATUS 0x%02X	809

Table A-8. Application Module—Error Log Messages (Continued)

ID	Log Message	No.
41771	QLBI_GetLunList: Lun allocation failed for LunId %d	811
41994	QLFC_Login: VpIndex (%d) out of range	1034
41995	QLFC_Login: VP Index 0x%x not configured	1035
42002	QLFC_Login: Can't open connection	1042
42024	QLFC_Logout: No active path to device. WWPN: %.2X%.2X%.2X%.2X%.2X%.2X%.2X%.2X	1064
42027	QLFC_Logout: VP Index 0x%x not configured	1067
42068	QLFC_HandleTeb: System Error	1108
42069	QLFC_HandleTeb: Driver Fatal Error	1109
42072	QLFC_HandleTeb: FC Logout	1112
42242	QLIS_AllocateSessionObject: Out of session resources	1282
42252	QLIS_EnqueueiScsiPdu: Duplicate PDU, CmdSN %d (0x%x), dropping it	1292
42258	QLIS_InstantiateSession: Can't add Initiator to the database	1298
42404	QLIS_ProcessStartTrb: [%d] CmdSN %ld is out of range (%ld - %ld), Cdb[0] 0x%02X, DataXferLen 0x%x.	1444
42648	QLIS_HandleTeb: Driver Fatal Error	1688
42649	QLIS_HandleTeb: Unload Driver	1689
42654	QLIS_HandleTeb: iSNS Connection Failed	1694
43012	QLSC_CollectBUVUIO: Allocation of DSD failed	2052
43013	QLSC_CollectBUVUIORecover: Allocation of DSD failed	2053
43265	QLUT_AllocateTpbExtension: TPB allocation failed	2305
43267	QLUT_AllocateTpbExtension: Data buffer allocation failed (length %d)	2307
43268	QLUT_AllocateTpbExtension: Alloc of DSD failed for buffer len %d	2308
43269	QLFCIP_IncomingFrame: BUGCHECK: Trb (0x%p) ValidFlag (0x%x) Direction (0x%x)	2309
43270	QLFCIP_IncomingFrame: GetFcipMapPortal failed	2310

Table A-8. Application Module—Error Log Messages (Continued)

ID	Log Message	No.
43271	QLFCIP_IncomingFrame: Got Status aborted pTrb->pBufDescList[0]:%p Trb Direction:0x%x	2311
43272	QLFCIP_SystemError: System error	2312
43273	QLFCIP_SystemError: QLOP_IssuePortEnable failed	2313
43280	QLFCIP_HandleTeb: Driver Fatal error	2320
43281	QLFCIP_ConfigPortal: Find portal object failed for QLUT_TYPE_FC, PortId (%d)	2321
43282	QLFCIP_ConfigPortal: QLFCIP_ConfigPortal: Invalid PortId for FCIP link PortID(%d)	2322
43283	QLUT_AllocateFcipTrbPool: Allocation failed (size 0x%x))	2323
43284	QLUT_GetFcipTrb: Null portal object in map table	2324
43285	QLUT_GetFcipTrb: Unable to get the Free Trb	2325
43286	QLUT_GetFcipTrb: Duplicate allocation of FcipTrb (0x%p)	2326
43287	QLUT_FreeFcipTrb: Null portal object in map table	2327
43288	QLUT_FreeFcipTrb: Duplicate Free of FcipTrb (0x%p)	2328
43289	QLUT_InitializeFcipBufDescPool: Memory allocation for FCIP_BUF_EXT_DESC failed (size 0x%x)	2329
43296	QLUT_FreeFcipDataBuffers: Duplicate Freeing of DataBuf (0x%p)	2336
43297	QLUT_AllocateFcipDataBuffers: Duplicate allocation of DataBuffer (0x%p)	2337
43298	QLUT_AllocateFcipDataBuffer: Got NULL PORTAL Object in map table MEM LEAK!!!!!	2338
43299	QLUT_DeallocateFcipDataBuffer: Null portal object in map table	2339
43300	QLUT_CreateFcipDataBufferpool: Allocation of 32K buffers from LargeBufferPool failed	2340
43521	QLSC_BreakupVUIOAllocPhase: TPB allocation failed	2561
43522	QLSC_BreakupVUIOAllocPhase: Data buffer and TPB allocation failed	2562

7	NULL doorbell routine for unloaded drivers. When a driver is unloaded, the doorbell routine is redirected to this NULL routine.
36	Processing unsupported ordered tag task management command.
44	Processing unsupported head-of-queue task management command.
98	Unable to create an object for the target device: exceeded the maximum number of target devices.
100	Unable to create an object for the target node: exceeded the maximum number of target devices.
107	Memory unavailable for LUN object.
117	Unable to create an object for initiator object: exceeded the maximum number of initiators.
136	Process control block status indicates that a PCI error occurred during a target operation.
146	Process control block status indicates that a DMA error occurred during an initiator operation.
147	Process control block status indicates that a transport error (protocol) occurred during an initiator operation.
151	Process control block status indicates that a data overrun error occurred during an initiator operation.
274	iSCSI login failed between receipt of PDU and request for the data segment.
278	iSCSI login failed due to unsupported version number in received login PDU.
297	iSCSI Login PDU contains invalid initiator name. The format and character set used to form the initiator name is invalid.
305	iSCSI target login was attempted to a portal (iSCSI1 or iSCSI2) on which the target is not presented.
307	iSCSI Login PDU received for a target with a target name unknown to the router.
308	iSCSI Login PDU received without a target name for a normal session.
310	iSCSI Login PDU received without an initiator name key/value.
312	iSCSI Login PDU received with an incorrect initiator task tag for a session which is partially logged in. This would occur if a login PDU other than the initial login PDU used an initiator task tag which was different than the initiator task tag provided in the initial login PDU.

323	iSCSI Login PDU was received with a TSIH out of range. This would occur if the iSCSI initiator attempting the login failed to used the TSIH value provided in the Target Login Response PDU (router is target) in subsequent login PDUs.
324	iSCSI Login PDU was received with an invalid TSIH value. The TSIH is invalid because there is no session with that TSIH value. This would occur if the iSCSI initiator attempting the login failed to used the TSIH value provided in the target login response PDU (router is target) in subsequent login PDUs.
393	CHAP validation failed during login.
394	Unexpected CHAP key.
548	Failed to allocate an object for *Set Port Info* IOCTL processing: PortType: 0 = FC, 1 = iSCSI PortId: 0 = FC1 or iSCSI1(GE1), 1 = FC2 or iSCSI2 (GE2)
666	Inquiry command failed. The Inquiry command was issued by the router as part of its discovery process.
669	Pass-Through command for Inquiry command for page 83 failed. The Inquiry command was issued by the router as part of its discovery process.
675	Pass-Through command for Read Capacity command failed. The Read Capacity command was issued by the router as part of its discovery process.
676	Read Capacity command failed. The Read Capacity command was issued by the router as part of its discovery process.
736	Pass-Through command issued by management application (such as the SANsurfer Router Manager) was aborted.
740	Pass-Through command issued by management application (such as the SANsurfer Router Manager) failed due to invalid CDB length.
741	Pass-Through command issued by management application (such as the SANsurfer Router Manager) failed due to invalid data length.
757	Pass-Through command issued by management application (such as the SANsurfer Router Manager) was interrupted or timed out.
790	IOCTL operation unsupported. Operation code provided in log message.
808	Report LUNs command failed. The Report LUNs command was issued by the router as part of its discovery process.
809	Report LUNs command failed with check condition status. The Report LUNs command was issued by the router as part of its discovery process.
811	Failed to allocate LUN object: out of resources.

1034	Login attempted using Fibre Channel virtual port (VP) index that is out-of-range (range = 0–31). Index reported in log message.
1035	Login attempted using Fibre Channel VP index that has not been configured. Operation attempted on an unconfigured VP.
1042	Attempting login but Fibre Channel connection cannot be opened.
1064	Attempting logout of device for which there is no active path (WWPN not found).
1067	Logout attempted using Fibre Channel VP index that has not been configured. Operation attempted on an unconfigured VP.
1108	Event notification: Fibre Channel processor encountered a system error (unrecoverable firmware error).
1109	Event notification: Fibre Channel driver encountered a fatal error.
1112	Event notification: Fibre Channel port logged out.
1282	Failed to allocate object for iSCSI session: out of session resources.
1292	Received iSCSI PDU with duplicate command sequence number (CmdSN). Command PDU will be dropped.
1298	Unable to allocate iSCSI initiator object while instantiating session.
1444	Failed to execute iSCSI Command PDU because its CmdSN is out-of-range. Log message contains the incorrect CmdSN, the valid CmdSN range, the first byte of the CDB, and the data length.
1688	Event notification: iSCSI driver encountered a fatal error.
1689	Event notification: an IOCTL request was received to unload the iSCSI driver.
1694	Event notification: attempt to connect to the iSNS server failed.
2052	iSNS connection failed.
2053	Break up I/O DSD allocation failed.
2305	Break up I/O recover DSD allocation failed.
2307	Data buffer allocation failed (length %d) during tpb extension allocation.
2308	Allocation of DSD failed during Tpb extension allocation. Buffer length %d.
2309	FCIP incoming frame: BUGCHECK: Trb (0x%p) ValidFlag (0x%x) Direction (0x%x).
2310	FCIP incoming frame: GetFcipMapPortal failed.

2311	FCIP incoming frame: Got Status aborted pTrb->pBufDescList[0]:%p Trb Direction:0x%x.
2312	FCIP system error.
2313	FCIP system error: QLOP_IssuePortEnable failed.
2320	FCIP handle Teb: Driver Fatal error.
2321	FCIP configure portal: Find portal object failed for QLUT_TYPE_FC, PortId (%d).
2322	FCIP configure portal: QLFCIP_ConfigPortal: Invalid PortId for FCIP link PortID(%d).
2323	FCIP allocate TRB pool: Allocation failed (size 0x%x).
2324	FCIP Trb: Null portal object in map table.
2325	FCIP get TRB: Null portal object in map table.
2326	FCIP get TRB: Duplicate allocation of FcipTrb (0x%p).
2327	FCIP free TRB: Null portal object in map table.
2328	FCIP free TRB: Duplicate Free of FcipTrb (0x%p).
2329	FCIP initialize buffer descriptor pool: memory allocation for FCIP_BUF_EXT_DESC failed (size 0x%x).
2336	FCIP free data buffers: Duplicate Freeing of DataBuf (0x%p).
2337	FCIP allocate data buffers: Duplicate allocation of DataBuffer (0x%p).
2338	FCIP allocate data buffer: Got NULL PORTAL Object in map table MEM LEAK.
2339	FCIP de-allocate data buffer: Null portal object in map table.
2340	FCIP create data buffer pool: Allocation of 32K buffers from LargeBufferPool failed.
2561	Break up I/O: TPB allocation failed.
2562	Break up I/O: Data buffer and TPB allocation failed.

iSCSI Driver

The following error log messages are common to both iSCSI ports, 1 (GE1) and 2 (GE2). They are listed in Table A-9 and described following the table. Log messages beginning with #0 denote iSCSI port 1 (GE1). Log messages beginning with #1 denote iSCSI port 2 (GE2).

Table A-9. iSCSI Driver—Error Log Messages

ID	Log Message	No.
73990	#%d: QLUtmIoctlEnable: Initialize FW failed	262
74046	#%d: QLPortUp: MBOX_CMD_SET_PORT_CONFIG %04x failed %04x	318
74056	#%d: QLRunDiag: MBOX Diag test internal loopback failed %x %x	328
74057	#%d: QLRunDiag: MBOX Diag test external loopback failed %x %x	329
74065	#%d: QLPortDown: MBOX_CMD_SET_PORT_CONFIG %04x failed %04x	337
74241	#%d: QLiSNSEnableCallback: iSNS Server TCP Connect failed	513
74577	#%d: QLIsrDecodeMailbox: NVRAM invalid	849
74587	#%d: QLIsrDecodeMailbox: Link down	859
74656	#%d: QLReadyTimer: Adapter missed heartbeat for %d seconds. Time left %d	928
74661	#%d: QLTimer: Abort pTpb=%p, Type %x, Timeout 0x%x DrvCount 0x%x, DdbIndex 0x%x	933
74663	#%d: QLReadyTimer: MBOX_CMD %04x %04x %04x %04x %04x %04x %04x %04x timed out	935
74665	#%d: QLReadyTimer: QLiSNSReenable failed	937
74784	#%d: QLUpdateInitiatorData: No more room in Initiator Database	1056
74800	#%d: QLSetTargetData: No more room in Target Database	1072

262	The iSCSI processor failed firmware initialization.
318	The iSCSI processor command to enable a GE port failed.
328	The iSCSI processor failed the internal loopback test.

329	The iSCSI processor failed the external loopback test.
337	The iSCSI processor command to disable a GE port failed.
513	The iSCSI processor could not connect with the iSCSI name server (iSNS).
849	The iSCSI processor reported that the iSCSI port NVRAM contains invalid data (checksum error).
859	The iSCSI processor reported a link down condition.
928	The driver failed to receive a heartbeat from the iSCSI processor for the specified number of seconds.
933	The driver timed out an iSCSI processor operation and is aborting the operation.
935	The driver timed out an iSCSI processor mailbox command.
937	The driver timed out while attempting to reconnect with the iSNS.
1056	The driver's initiator database is full. The driver is capable of storing 1024 iSCSI initiators in its database. Use the CLI or the SANsurfer Router Manager to remove unwanted/unused iSCSI initiators.
1072	The driver's target database is full. Use the CLI or the SANsurfer Router Manager to remove unwanted/unused iSCSI targets.

Fibre Channel Driver

The following error log messages are common to both Fibre Channel ports, 1 (FC1) and 2 (FC2). They are listed in Table A-10 and described in this section. Log messages beginning with #0 denote Fibre Channel port 1 (FC1) and log messages beginning with #1 denote Fibre Channel port 2 (FC2).

Table A-10. Fibre Channel Driver—Error Log Messages

ID	Log Messages	No.
106583	#%d: QLUtmReceiveIo: Path invalid/FW No resource count %x	87
106589	#%d: QLIoctlEnable: Adapter disabled	93
106590	#%d: QLIoctlEnable: Initialize FW error	94
106592	#%d: QLIoctlRunDiag: Diagnostic loopback command failed %x % %x %x	96
106593	#%d: QLIoctlDisable: Re-initialize adapter failed	97
106595	#%d: QLUtmReceiveIo: Invalid VP Loop Id 0x%x	99
106803	#%d: QLIsrEventHandler: Link down (%x)	307
106813	#%d: QLIsrEventHandler: Unexpected async event (%x), MB1=%x, MB2=%x, MB3=%x, MB4=%x, MB5=%x, MB6=%x, MB7=%x	317
106846	#%d: QLProcessResponseQueueFS: TRB is NULL: %d	350
106853	#%d: QLTimer: Link error count (0x%x) exceeded, link down	357
106912	#%d: QLReserveLoopId: out of loop Ids	416
106928	#%d: QLMarkDeviceOffline: Device Id: %x marked offline, cLinkDownTimeout = %x, cPortDownRetryCount=%x	432
106948	#%d: QLSnsGetAllNext: Name server login FAILED %x	452
107029	#%d: QLUpdateDeviceData: out of slots in host database	533
107030	#%d: QLUpdateDeviceData: out of slots in target database	534
107041	#%d: QLUpdateDeviceDatabase 0x%x: GET_ID failed %x	545
107056	#%d: QLUpdateDeviceDatabase 0x%x: out of slots in host database	560
107058	#%d: QLUpdateDeviceDatabase 0x%x: MBOX_CMD_GET_VP_DATABASE failed %x	562
107078	#%d: QLUpdatePort 0x%x: out of slots in host database	582

Table A-10. Fibre Channel Driver—Error Log Messages (Continued)

ID	Log Messages	No.
107254	#%d: QLUpdateSinglePortCont 0x%x: out of slots in host database	758
107267	#%d: QLFcipIsrEventHandler: System error event (%x), MB1=%x, MB2=%x, MB3=%x, MB4=%x, MB5=%x, MB6=%x, MB7=%x	771

87	The FC processor received a SCSI command for an unknown target path or has run out of resources to execute additional commands.
93	The FC processor was disabled by an IOCTL request to the driver.
94	The FC processor firmware failed initialization. The request to initialize was received by the driver in an IOCTL request.
96	The FC processor failed the external loopback test.
97	The FC processor failed to re-initialize in response to an IOCTL disable request.
99	Invalid Virtual Port loop ID.
307	The FC processor reported a link down condition.
317	The FC processor reported an unexpected asynchronous event. The mailbox registers provide status, event code, and data related to the event.
350	FCIP Response queue entry TRB pointer is NULL.
357	The driver has determined that the FC link is unreliable and unusable due to the number of errors encountered. The link has been taken down.
416	The FC processor was unable to obtain the number of loop IDs required. This failure occurs only when the FC processor is running multi-ID firmware.
432	The driver was unable to re-establish connection to the target within the timeout and retry counts, and is therefore marking it *offline*.
452	The FC processor is unable to log into the FC fabric name server.
533	The driver’s host (initiator) database is full.
545	The driver’s target database is full.
560	The driver’s host (initiator) database is full. Maximum host database is 64.
562	FC processor "Get VP Database entry command" failed.

582	The drivers host (initiator) database is full.
758	No slots available in host database.
771	FCIP system error event.

User Modules

The user modules generate the error log messages listed in Table A-11 and described following the table.

Table A-11. User Modules—Error Log Messages

ID	Log Message	No.
139265	QBRPC_Initialize: Entered	1
139266	QBRPC_Initialize:GetBridge Mem Allocation error	2
139267	QBRPC_Initialize:GetBridgeAdv Mem Allocation error	3
139268	QBRPC_Initialize:GetMgmt Mem Allocation error	4
139269	QBRPC_Initialize:GetIscsi Mem Allocation error	5
139270	QBRPC_Initialize:GetIscsiAdv Mem Allocation error	6
139271	QBRPC_Initialize:GetIsns Mem Allocation error	7
139272	QBRPC_Initialize:GetFcIntfc Mem Allocation error	8
139273	QBRPC_Initialize:GetFcAdv Mem Allocation error	9
139280	QBRPC_Initialize:GetFcSfp Mem Allocation error	16
139281	QBRPC_Initialize:GetLog Mem Allocation error	17
139282	QBRPC_Initialize:GetStats Mem Allocation error	18
139283	QBRPC_Initialize:InitListMem Allocation error	19
139284	QBRPC_Initialize:TargetList Mem Allocation error	20
139285	QBRPC_Initialize:LunList MemAllocation error	21
139286	QBRPC_Initialize:PresTarget Mem Allocation error	22
139287	QBRPC_Initialize:LunMask Mem Allocation error	23
139288	QBRPC_Initialize:Init Mem Allocation error	24
139289	QBRPC_Initialize:TgtDevice Mem Allocation error	25
139296	QBRPC_Initialize:FcTgt Mem Allocation error	32

Table A-11. User Modules—Error Log Messages (Continued)

ID	Log Message	No.
139297	QBRPC_Initialize:BridgeStatus Mem Allocation error	33
139298	QBRPC_Initialize:Diag Mem Allocation error	34
139299	QBRPC_Initialize:DiagLog Mem Allocation error	35
139300	QBRPC_Initialize:FruImage Mem Allocation error	36
139301	QBRPC_Initialize:OemMfg Mem Allocation error	37
139302	QBRPC_Initialize:Status Mem Allocation error	38
139303	QBRPC_Initialize:TcpIpStats Mem Allocation error	39
139304	QBRPC_Initialize:NtpStats Mem Allocation error	40
139305	QBRPC_Initialize:LunList MemAlloc error	41
139315	QBRPC_FreeResources:Entered	51
139553	checkDuplicateIp: Detected Error %08x %08x%04x	289

1	RPC (remote procedure call) server initialization entry point.
2	Get System API memory allocation failed.
3	Get System Advanced API memory allocation failed.
4	Get Management API memory allocation failed.
5	Get iSCSI API memory allocation failed.
6	Get iSCSI advanced API memory allocation failed.
7	Get iSNS API memory allocation failed.
8	Get FC Interface API memory allocation failed.
9	Get FC Advanced API memory allocation failed.
16	Failed memory allocation for Get FC SFP API.
17	Failed memory allocation for Get Log API.
18	Failed memory allocation for Get Statistics API.
19	Failed memory allocation for Get Initiator List API.
20	Failed memory allocation for Get Target List API.

21	Failed memory allocation for Get LUN List API.
22	Failed memory allocation for Get Presented Targets List API.
23	Failed memory allocation for Get LUN Mask API.
24	Failed memory allocation for Initiator API.
25	Failed memory allocation for Target Device API.
32	Failed memory allocation for FC Target API.
33	Failed memory allocation for System Status API.
34	Failed memory allocation for Diagnostic API.
35	Failed memory allocation for Diagnostic Log API.
36	Failed memory allocation for FRU Image API.
37	Failed memory allocation for OEM Manufacturing API.
38	Failed memory allocation for Status API.
39	Failed memory allocation for TCP/IP Statistics API.
40	Failed memory allocation for NTP Status API.
41	Failed memory allocation for LUN List API.
51	RPC free resources entry point.
289	Detected duplicate IP address for management port.

System

The system modules generate the error log messages listed in Table A-12 and described following the table.

Table A-12. System—Error Log Messages

ID	Log Message	No.
237572	"Failed to kill sys killer %d\n"	4
237573	"Temperature over high threshold %d\n"	5

4	Failed to kill system task.
5	Reporting router exceeds maximum operating temperature.

Fatal Log Messages

The following sections list and describe the fatal log messages by reporting module:

- "iSCSI Driver" on page A-25
- "FC Driver" on page A-28
- "TOE Driver" on page A-30
- "System" on page A-31

iSCSI Driver

The following fatal log messages are common to both iSCSI ports, 1 (GE1) and 2 (GE2). They are listed in Table A-13 and described following the table. Log messages beginning with #0 denote iSCSI port 1 (GE1). Log messages beginning with #1 denote iSCSI port 2 (GE2).

Table A-13. iSCSI Driver—Fatal Log Messages

ID	Log Message	No.
69652	#%d: qlutm_init: Diagnostic failed, invalid SRAM	20
69653	#%d: qlutm_init: Diagnostic failed, fail reboot	21
69654	#%d: qlutm_init: Diagnostic failed, invalid NVRAM	22
69655	#%d: qlutm_init: Diagnostic failed, invalid DRAM	23
69656	#%d: qlutm_init: Failed to return diagnostic result to Bridge	24

Table A-13. iSCSI Driver—Fatal Log Messages (Continued)

ID	Log Message	No.
69941	#%d: QLUtmProcessResponseQueue: Invalid handle %x EntryType %x	309
69951	#%d: QLSetNvram: QLRebootTimer failed AF %x RS %x Time %d	319
69964	#%d: QLDisable: QLRebootTimer failed AF %x RS %x Time %d	332
69966	#%d: QLEnable: QLRebootTimer failed AF %x RS %x Time %d	334
70224	#%d: QLProcSrblessiSNSResponse: Invalid handle %x	592
70400	#%d: QLInitializeDevice: QLStartAdapter failed	768
70417	#%d: QLInitializeAdapter: QLInitializeFW failed	785
70432	#%d: QLDoInterruptServiceRoutine: PortFatal interrupt. PortFatalErrorStatus %08x CSR %08x AS %x AF %x	800
70448	#%d: QLStartAdapter: QLRebootTimer failed AF %x RS %x Time %d	816
70489	#%d: QLIsrDecodeMailbox: System Error 8002 MB[1-7] %04x %04x %04x %04x %04x %04x %04x	857
70499	#%d: QLProcessResponseQueue: Invalid handle for ET_PASSTHROUGH_STATUS	867
70501	#%d: QLProcessResponseQueue: Invalid entry type in response queue %x	869
70502	#%d: QLProcessResponseQueue: Invalid handle %x EntryType %x	870
70524	#%d: QLProcessAen: Invalid event %x	892
70544	#%d: QLRebootTimer: Reboot failed!	912
70563	#%d: QLReadyTimer: Adapter missed heartbeat for 0x%x seconds. Rebooting	931
70564	#%d: QLReadyTimer: Abort pTpb=%p failed, DrvCount 0x%x	932
70609	#%d: QLProcessSystemError: Restart RISC	977
70610	#%d: QLProcessSystemError: RebootHba failed	978
70784	#%d: QLConfigChip: invalid NVRAM	1152
70835	#%d: QLStartFw: MBOX_CMD_SET_FLASH failed %x	1203

Table A-13. iSCSI Driver—Fatal Log Messages (Continued)

ID	Log Message	No.
70836	#%d: QLStartFw: Invalid Fw loader state 0x%x	1204
70837	#%d: QLStartFw: Load Fw loader timeout	1205

20	iSCSI processor SRAM test failed.
21	iSCSI processor failed diagnostic reboot.
22	iSCSI processor failed NVRAM diagnostic.
23	iSCSI processor failed DRAM diagnostic.
24	iSCSI processor failed to return diagnostic results.
309	Response queue entry contains an invalid handle.
319	Set NVRAM reboot timer failed.
332	Port disable reboot timer failed.
334	Port enable reboot timer failed.
592	iSNS response contains an invalid handle.
768	Start iSCSI processor failed.
785	iSCSI processor firmware initialization failed.
800	iSCSI processor port fatal error.
816	Start iSCSI processor reboot timer failed.
857	iSCSI processor fatal system error.
867	Response queue invalid handle for ET pass-through.
869	Response queue invalid entry type.
870	Response queue invalid handle for specified entry type.
892	Asynchronous event for unknown event type.
912	Reboot timer failed.
931	iSCSI driver missed iSCSI processor heartbeat. iSCSI processor rebooted.
932	iSCSI processor failed to complete operation before timeout.
977	iSCSI processor system error restart.

978	iSCSI processor reboot failed.
1152	iSCSI processor NVRAM invalid (checksum error).
1203	iSCSI FLASH (NVRAM) command failed.
1204	iSCSI firmware loader invalid state.
1205	iSCSI failed to load firmware in time allotted.

FC Driver

The following fatal log messages are common to both Fibre Channel ports, 1 (FC1) and 2 (FC2). They are listed in Table A-14 and described following the table. Log messages beginning with #0 denote Fibre Channel port 1 (FC1). Log messages beginning with #1 denote Fibre Channel port 2 (FC2).

Table A-14. Fibre Channel Driver—Fatal Log Messages

ID	Log Message	No.
102419	#%d: qlutm_init: Diagnostic failed, port 1 invalid SRAM	19
102420	#%d: qlutm_init: Diagnostic failed, port 1 POST failed	20
102421	#%d: qlutm_init: Diagnostic failed, port 2 invalid SRAM	21
102422	#%d: qlutm_init: Diagnostic failed, port 2 POST failed	22
102423	#%d: qlutm_init: Failed to return diagnostic result to Bridge	23
102656	#%d: QLInitializeAdapter: Reset ISP failed	256
102657	#%d: QLInitializeAdapter: Load RISC code failed	257
102658	#%d: QLInitializeAdapter: Load ISP2322 receive sequencer code failed	258
102659	#%d: QLInitializeAdapter: Load ISP2322 transmit sequencer code failed	259
102662	#%d: QLInitializeAdapter: Verify Checksum command failed (%x)	262
102680	#%d: QLInitializeFW: FAILED	280
102688	#%d: QLInterruptServiceRoutine: Risc pause %x with parity error hccr %x, Disable adapter	288
102689	#%d: QLInterruptServiceRoutine: Invalid interrupt status: %x	289
10691	#%d: QLFcipInterruptServiceRoutine: Risc pause %x with parity error hccr %x, Disable adapter	291

Table A-14. Fibre Channel Driver—Fatal Log Messages (Continued)

ID	Log Message	No.
10692	#%d: QLFcipInterruptServiceRoutine: Invalid interrupt status: %x	292
102716	#%d: QLIsrEventHandler: System error event (%x), MB1=%x, MB2=%x, MB3=%x, MB4=%x, MB5=%x, MB6=%x, MB7=%x	316
102746	#%d: QLProcessResponseQueue: Invalid handle %x, type %x	346
102747	#%d: QLProcessResponseQueueFS: Invalid buffer type: %x	347
102748	#%d: QLProcessResponseQueueFS: Invalid EntryType (0x%x)	348
102749	#%d: QLProcessResponseQueueFS: Invalid handle 0x%x, type 0x%x	349
102752	#%d: QLTimer: Ext Ram parity error exceed limit cnt 0x%x, limit 0x%x, Disabled adapter	352
102755	#%d: QLTimer: Heartbeat failed	355
102800	#%d: QLRestartRisc: restart RISC	400

19	FC1 processor SRAM test failed.
20	FC1 processor power-on self-test (POST) failed.
21	FC2 processor SRAM test failed.
22	FC2 processor POST failed.
23	FC processor failed to return diagnostic results.
256	FC processor failed reset.
257	FC processor firmware load failed.
258	FC processor receive sequencer code load failed.
259	FC processor transmit sequencer code load failed.
262	FC processor firmware checksum failed.
280	FC processor firmware initialization failed.
288	FC processor paused due to internal parity error.
289	FC processor returned an invalid interrupt status.
291	FC processor invalid interrupt status.

292	FC processor paused due to RAM parity error.
316	FC processor system error.
346	Response queue entry contains an invalid handle.
347	FCIP: Response queue entry contains an invalid buffer type.
348	FCIP: Response queue entry contains an invalid entry type.
349	FCIP: Response queue entry contains an invalid handle.
352	FC processor external SRAM parity error count exceeded limit: FC port disabled.
355	FC processor heartbeat failed.
400	FC processor being restarted.

TOE Driver

The TOE driver generates the fatal log messages listed in Table A-15 and described following the table.

Table A-15. TOE—Fatal Log Messages

ID	Log Message	No.
200721	QL3022:ql3xxx_probe: Adapter eth#%d, Invalid NVRAM parameters	17
200725	QL3022:eth%x: Resetting chip. PortFatalErrStatus register = 0x%x	21

17	Encountered invalid parameters in TOE NVRAM.
21	TOE chip reset due to detection of fatal error.

System

The system modules generate the fatal log messages listed in Table A-16 and described following the table.

Table A-16. System—Fatal Log Messages

ID	Log Message	No.
233473	"memory monitor: Detected Uncorrectable Ecc %08lx system is rebooting in 5 secs\n"	1
233474	"Failed to register interrupt handler!\n"	2
233475	"%s class_simple_create failed\n"	3

1	Uncorrectable memory error detected at address provided in log message.
2	Attempt to register the interrupt handler failed.
3	Failed class_simple_create system call from memory monitor initialization routine.

Notes

B Simple Network Management Protocol (SNMP)

Introduction

Simple network management protocol (SNMP) provides monitoring and trap functions for managing the router through third-party applications that support SNMP. The router firmware supports SNMP versions 1 and 2 and a QLogic (see page B-3). You may format the traps using SNMP version 1 or 2 (see page B-11).

SNMP Properties

You can set the SNMP properties using the SANsurfer Router Manager (see "SNMP Management Tab" on page 3-7).

Table B-1 describes the SNMP properties.

Table B-1. SNMP Properties

Parameter	Description
Read community	A password that authorizes an SNMP management server to read information from the router. This is a write-only field. The value on the router and the SNMP management server must be the same. The read community password can be up to 32 characters *excluding* the number sign (#), semicolon (;), and comma (,). The default is password is *public*.
Trap community	A password that authorizes an SNMP management server to receive traps. This is a write-only field. The value on the router and the SNMP management server must be the same. The trap community password can be up to 32 characters *excluding* the number sign (#), semicolon (;), and comma (,). The default password is *public*.
System location	Specifies the name of the router location. The name can be up to 64 characters *excluding* the number sign (#), semicolon (;), and comma (,). The default is undefined.

Table B-1. SNMP Properties (Continued)

Parameter	Description
System contact	Specifies the name of the person to be contacted to respond to trap events. The name can be up to 64 characters *excluding* the number sign (#), semicolon (;), and comma (,). The default is undefined.
Authentication traps	Enables or disables authentication trap generation in response to authentication failures. The default is disabled.

SNMP Trap Configuration

SNMP trap configuration supports setting up to eight trap destinations. Choose from Traps 1–Trap 8 to configure each trap. Table B-2 describes the parameters for configuring a SNMP trap.

Table B-2. SNMP Trap Configuration Parameters

Parameter	Description
Trap *n* enabled	Enables or disables trap *n*. If disabled, the trap is not configured.
Trap address*	Specifies the IP address to which the SNMP traps are sent. A maximum of eight trap addresses are supported. The default address for traps is 0.0.0.0.
Trap port*	The port number on which the trap is sent. The default is 162.
Trap version	Specifies the SNMP version (1 or 2) with which to format traps.

*Trap address (other than 0.0.0.) and trap port combinations must be unique. For example, if trap 1 and trap 2 have the same address, then they must have different port values. Similarly, if trap 1 and trap 2 have the same port value, they must have different addresses.

Management Information Base (MIB)

The following sections describe the QLogic management information base (MIB). The MIB consists of four object groups:

- System Information
- Network Port Table
- Fibre Channel Port Table
- Fibre Channel Port Table

System Information

The system information objects provide the system serial number, version numbers (hardware/software/agent), and number of ports (FC/GE).

qsrSerialNumber

Syntax	SnmpAdminString
Access	Read only
Description	The system serial number.

qsrHwVersion

Syntax	SnmpAdminString
Access	Read only
Description	The system hardware version number.

qsrSwVersion

Syntax	SnmpAdminString
Access	Read only
Description	The system software (firmware) version number.

qsrNoOfFcPorts

Syntax	Unsigned32
Access	Read only
Description	The number of Fibre Channel ports on the system.

qsrNoOfGbEPorts

Syntax	Unsigned32
Access	Read-only
Description	The number of gigabit Ethernet ports on the system.

qsrAgentVersion

Syntax	SnmpAdminString
Access	Read only
Description	The version number of the agent software on the system.

Network Port Table

The network port table contains a list of network ports that are operational on the router. The entries in this table include the management port, the iSCSI ports, and the TOE ports on the router. A single gigabit Ethernet port can function as an iSCSI port and a TOE simultaneously; therefore, there may be up to two entries for a given gigabit Ethernet port.

qsrNwPortTable

Syntax	**Sequence of** QsrNwPortEntry
Access	Not accessible
Description	The entries in this table include the management port, and the iSCSI, and TOE ports on the router.

qsrNwPortEntry

Syntax	QsrNwPortEntry
Access	Not accessible
Description	Each entry (row) contains information about a specific network port.

QsrNwPortEntry

A network port entry consists of the following sequence of objects:

qsrNwPortRole	QsrPortRole
qsrNwPortIndex	unsigned32
qsrNwPortAddressMode	INTEGER
qsrIPAddressType	InetAddressType
qsrIPAddress	InetAddress

qsrNetMask	InetAddress
qsrGateway	InetAddress
qsrMacAddress	MacAddress
qsrNwLinkStatus	QsrLinkStatus
qsrNwLinkRate	QsrLinkRate

qsrNwPortRole

Syntax	QsrPortRole
Access	Not accessible
Description	The operational role of this port: management port, iSCSI port, a TOE.

qsrNwPortIndex

Syntax	Unsigned32
Access	Not accessible
Description	A positive integer indexing each network port in a given role.

qsrNwPortAddressMode

Syntax	INTEGER 1 = Static 2 = DHCP 3 = Bootp 4 = RARP
Access	Read only
Description	The method by which the port gets its IP address.

qsrIPAddressType

Syntax	InetAddressType
Access	Read only
Description	The IP address type: ipv4 or ipv6.

qsrIPAddress

Syntax	InetAddress
Access	Read only
Description	The IP address of the port.

qsrNetMask

Syntax	InetAddress
Access	Read only
Description	The subnet mask for this port.

qsrGateway

Syntax	InetAddress
Access	Read only
Description	The gateway for this port.

qsrMacAddress

Syntax	IMacAddress
Access	Read only
Description	The MAC address for this port.

qstNwLinkStatus

Syntax	QsrLinkStatus
Access	Read only
Description	The operational link status for this port.

qsrNwLinkRate

Syntax	QsrLinkRate
Access	Read only
Description	The operational link rate for this port.

Fibre Channel Port Table

This table contains a list of the Fibre Channel (FC) ports on the router.There are as many entries in this table as there are FC ports on the router.

qsrFcPortTable

Syntax	**Sequence of** QsrFcPortEntry
Access	Not accessible
Description	A list of the FC ports on the router.There are as many entries in this table as there are FC ports on the router.

qsrFcPortEntry

Syntax	QsrFcPortEntry
Access	Not accessible
Description	Each entry (row) contains information about a specific FC port.

QsrFcPortEntry

A Fibre Channel port entry consists of the following sequence of objects:

qsrFcPortRole	QsrPortRole
qsrFcPortIndex	Unsigned32
qsrFcPortNodeWwn	PhysAddress
qsrFcPortWwn	PhysAddress
qsrFcPortId	PhysAddress
qsrFcPortType	Unsigned32
qsrFcLinkStatus	QsrLinkStatus
qsrFcLinkRate	QsrLinkRate

qsrFcPortRole

Syntax	QsrPortRole
Access	Not accessible
Description	The operational role of this port: FCP mode or frame shuttle mode.

qsrFcPortIndex

Syntax	Unsigned32
Access	Not accessible
Description	A positive integer indexing each FC port in a given role.

qsrFcPortNodeWwn

Syntax	PhysAddress
Access	Read only
Description	The world-wide name of the node that contains this port.

qsrFcPortWwn

Syntax	PhysAddress
Access	Read only
Description	The world-wide name for this port.

qsrFcPortId

Syntax	PhysAddress
Access	Read only
Description	The interface's 24-bit FC address identifier.

qsrFcPortType

Syntax	Unsigned32
Access	Read only
Description	The type of FC port, as indicated by the use of the appropriate value assigned by IANA. The IANA-maintained registry for FC port types can be found at: www.iana.org/assignments/fc-port-types

qsrFcLinkStatus

Syntax	QsrLinkStatus
Access	Read only
Description	The current link status for this port.

qsrFcLinkRate

Syntax	QsrLinkRate
Access	Read only
Description	The current link rate for this port.

Sensor Table

This table contains a list of all the sensors on the router. There are as many entries (rows) in this table as there are sensors.

qsrSensorTable

Syntax	**Sequence of** QsrSensorEntry
Access	Not accessible
Description	A list of all the sensors on the router. There are as many entries (rows) in this table as there are sensors.

qsrSensorEntry

Syntax	QsrSensorEntry
Access	Not accessible
Description	Each entry (row) corresponds to a single sensor.

QsrSensorEntry

A sensor entry consists of the following sequence of objects:

qsrSensorType	INTEGER
qsrSensorIndex	Unsigned32
qsrSensorUnits	INTEGER
qsrSensorValue	Integer32
qsrUpperThreshold	Integer32
qsrLowerThreshold	Integer32
qsrSensorState	INTEGER

qsrSensorType

Syntax	INTEGER Temperature = 1
Access	Not accessible
Description	The type of data being measured by this sensor.

qsrSensorIndex

Syntax	Unsigned32
Access	Not accessible
Description	A positive integer identifying each sensor of a given type.

qsrSensorUnits

Syntax	INTEGER Celsius = 1
Access	Read only
Description	The unit of measurement for the sensor.

qsrSensorValue

Syntax Integer32

Access Read only

Description The current value of the sensor.

qsrUpperThreshold

Syntax Integer32

Access Read only

Description The upper-level threshold for this sensor.

qsrLowerThreshold

Syntax Integer32

Access Read only

Description The lower-level threshold for this sensor.

qsrSensorState

Syntax INTEGER

Access Read only

Description The state of this sensor, indicating the health of the system.

- **Unknown –** The sensor value/thresholds cannot be determined.
- **Normal –** The sensor value is within normal operational limits.
- **Warning –** The sensor value is approaching a threshold.
- **Critical –** The sensor value has crossed a threshold.

Notifications

The router provides the following notification types:

- Notification Objects
- Agent Start Up Notification
- Agent Shut Down Notification
- Network Port Down Notification
- Fibre Channel Port Down Notification
- Sensor Notification
- Generic Notification

The following sections describe these notifications and objects they use.

Notification Objects

This section defines the objects used in notifications.

qsrEventSeverity

Syntax	INTEGER
Access	Accessible for notify
Description	This notification indicates the severity of the event. The value *clear* specifies that a condition that caused an earlier trap is no longer present.

qsrEventDescription

Syntax	SnmpAdminString
Access	Accessible for notify
Description	A textual description of the event that occurred.

qsrEventTimeStamp

Syntax	DateAndTime
Access	Accessible for notify
Description	This notification indicates when the event occurred.

Agent Start Up Notification

The agent startup notification indicates that the agent on the router has started running.

qsrAgentStartup uses the following object:

- qsrEventTimeStamp

Agent Shut Down Notification

The agent shut down notification indicates that the agent on the router is shutting down.

qsrAgentShutdown uses the following object:

- qsrEventTimeStamp

Network Port Down Notification

The network port down notification indicates that the specified network port is *down*. The next time the port comes up, this event is sent with the *qsrEventSeverity* object set to *clear*.

qsrNwPortDown uses the following objects:

- qsrNwLinkStatus
- qsrEventTimeStamp
- qsrEventSeverity

Fibre Channel Port Down Notification

The Fibre Channel port down notification indicates that the specified Fibre Channel port is *down*. The next time the port comes up, this event is sent with the *qsrEventSeverity* object set to *clear*.

qsrFcPortDown uses the following objects:

- qsrFcLinkStatus
- qsrEventTimeStamp
- qsrEventSeverity

Sensor Notification

The sensor notification indicates that the state for the specified sensor is not *normal*. When the sensor returns to the normal state, this event is sent with the *qsrEventSeverity* object set to *clear*.

qsrSensorNotification uses the following objects:

- qsrSensorValue
- qsrSensorState
- qsrEventTimeStamp
- qsrEventSeverity

Generic Notification

The generic notification reports events other than the defined event types. It provides a description object that identifies the event in clear text.

qsrGenericEvent uses the following objects:

- qsrEventTimeStamp
- qsrEventSeverity
- qsrEventDescription

Notes

Index

A

Action menu 2-3, 2-8
Add Initiator Wizard 2-5
  menu option 2-9
  procedures 4-7
Add Remote Router Wizard 2-6
  menu option 2-9
  procedures 4-25
Advanced configuration
  FC port 3-12
  iSCSI ports 3-18
Application
  error log A-10
  log messages A-2

B

Bandwidth, FCIP routes 3-32
Base name, iSCSI ports 3-15
Beacon
  OFF 2-9
  ON 2-9
Bi-directional CHAP configuration 5-2, 5-3
Broadcast 2-4
  enabling 2-5
  interval 2-5
Browser location 2-7
Burst length, iSCSI ports 3-19

C

CHAP
  configuration 5-1
  iSCSI port settings 3-20
Community
  read B-1
  trap B-1
Compression, FCIP routes 3-32
Configuration 2-3
  SNMP 3-7
Configuration Wizard
  menu option 2-5
  procedures 4-2
Connect
  icon 2-7
  menu option 2-8
Connection mode 3-12
Contact information 1-3

D

Data digest, iSCSI ports 3-19
Data rate, FC port 3-12
Disconnect, menu option 2-8
Discover iSCSI Target
  menu option 2-9
  procedures 4-42
Discover iSCSI Target Wizard 2-6
Discovered
  FC targets 3-25
  iSCSI initiators 3-22
  iSCSI targets 3-29

E

Error
  detect timeout 3-32
  log messages A-10
Execution throttle, FC port 3-12

F

Fatal log messages A-25
FC
  discovered targets 3-25
  driver fatal log messages A-28
  link status, FCIP routes 3-31
  port advanced configuration 3-12
  port, FCIP routes 3-31
  port, MIB B-6
  ports 3-11
FCIP
  messages A-8
  routes, interface status 3-31
FCIP Route Add Wizard 2-6
  menu option 2-9
  procedures 4-45
FCIP Route Remove Wizard 2-6
  menu option 2-9
  procedures 4-51
Features, licensed 3-9
Fibre Channel
  driver messages A-5
  error log messages A-20
  port count 3-2
  ports 3-11
File menu 2-4
Flow control, iSCSI ports 3-15
Frame size, FC port 3-12
FRU, saving and restoring 2-4
FW Update Wizard 2-5
  menu option 2-9
  procedures 4-9

G

Gateway IP address, FCIP routes 3-31
GigE port
  FCIP routes 3-31
  flow control 3-32
GUI, configuring CHAP 5-2, 5-3, 5-4

H

Hardware
  remote router version 3-9
  router version 3-2
Header digest, iSCSI ports 3-19
Help menu 2-7

I

Information 2-3
  basic router 3-2
  FC port 3-11
  FC target 3-26
  iSCSI ports 3-14
  NTP server 3-5
  router 3-2
Initiator
  discovered 3-22
Interval, broadcast 2-5
Introduction 1-1
IPv4
  address, iSCSI ports 3-16
  management port 3-4
IPv6 3-5
  address, iSCSI ports 3-16
  management port 3-4
iSCSI
  discovered targets 3-29
  driver messages A-4, A-18
  error log messages A-18
  fatal log messages A-25
  port count 3-2, 3-9
  presented target 3-27
  presented targets 3-29
  targets, presented 3-27
iSCSI ports 3-14
  advanced configuration 3-18
  information 3-14
  network settings 3-16
  statistics 3-21
iSNS, iSCSI ports 3-17
iSR6142 Router 2-12, 3-1

J

Jumbo frames
  FCIP routes 3-31
  iSCSI ports 3-19

L

License, features tab 3-9
Link rate
  GigE 3-32
  iSCSI ports 3-15
  mode 3-15
  mode, FCIP routes 3-32
Link status
  FC port 3-11
  GigE 3-31
  iSCSI ports 3-15
  management port 3-3
Local
  IP address, FCIP routes 3-31
  presented target 3-23
Log
  data A-1
  messages A-1
Logs, viewing 2-4

M

MAC address
  iSCSI ports 3-15
  management port 3-3
Main window 2-2
Management
  IP address 3-9
  router information 3-3
  SNMP 3-7
Map Local Initiator/Target Wizard 2-6
  menu option 2-8
  procedures 4-13
Map Remote Initiator/Target Wizard 2-6
  menu option 2-9
  procedures 4-33
Menus
  Action 2-8
  File 2-4
  Help 2-7
  Settings 2-4
  View 2-4
  Wizards 2-5

Messages
102419-102748 A-28
1026-1027 A-3
102749-102800 A-29
1028-1061 A-3
1034-1035 A-16
1042-2313 A-16
1056-1072 A-19
106583-107078 A-20
107254-107267 A-21
109 A-3
1111 A-3
1120 A-3
1152-1205 A-28
118882 A-5
119088-119097 A-5
119552-119554 A-5
1-3 A-31
139265-139296 A-22
139297-139553 A-23
151842-151902 A-6
151903-152071 A-7
16-20 A-23
1690-2051 A-3
17-21 A-30
184524-184525 A-8
1-9 A-23
19-23 A-29
200721-200725 A-30
20-24 A-27
204-205 A-8
21-51 A-24
217350 A-9
233473-233475 A-31
237572-237573 A-25
249862 A-9
256-349 A-29
262 A-9, A-18
289 A-24
290-347 A-7
304-313 A-5
307-562 A-21
309-978 A-27
318 A-18
324-809 A-15
327-358 A-4
328 A-18
329-937 A-19
348-359 A-8
352-400 A-30
36 A-14
40967-41268 A-10
41270-42002 A-11
42024-43273 A-12
43280-43522 A-13
44 A-14
4-5 A-25
517-519 A-8
53254-54277 A-2
54306-55299 A-2
582-771 A-22
6 A-3, A-9
69652-69951 A-25
69964-70837 A-26
7 A-14
73990-74800 A-18
768-770 A-6
86343-86874 A-4
87-99 A-21
98 A-5
98-323 A-14
application A-2
error log A-10
fatal log A-25
FCIP A-8
Fibre Channel driver A-5
informational A-1
iSCSI driver A-4, A-18
log A-1
system A-9
TOE driver A-9
user modules A-6

MIB
  Fibre Channel ports B-6
  network ports B-4
  notifications B-11
  objects B-3
  sensors B-8
  system B-3

N

Network
  ports, MIB B-4
  settings, iSCSI ports 3-16
Node name, FC port 3-11
Notification
  agent shut down B-12
  agent start up B-12
  FC port down B-12
  generic B-13
  MIB B-11
  network port down B-12
  objects B-11
  sensor B-13
NTP, server information 3-5
Number, iSCSI ports 3-18

P

Password 3-6
Performance, FC port 3-13
Ping, menu option 2-8
Port
  count, iSCSI 3-9
  FC 3-11
  ID, FC port 3-11
  name, FC port 3-11
Presented
  iSCSI target 3-27
  local target 3-23
  remote devices 3-26
  remote target 3-24
Product name
  remote router 3-9
  router 3-2
Programmed link rate 3-15
Properties, SNMP B-1

R

Read community B-1
Reboot, menu option 2-8
Refresh
  icon 2-7
  menu option 2-8
  statistics 3-21
Related materials 1-1
Remote
  assigned router 3-9
  IP address, FCIP routes 3-31
  presented devices 3-26
  presented target 3-24
Remove
  Initiator, menu option 2-9
  offline target, menu option 2-9
Remove Remote Router Wizard 2-6
  menu option 2-9
  procedures 4-30
Resource allocate, timeout 3-32
Restoring FRU 2-4
Router
  information 3-2
  iSR6142 2-12, 3-1
  security tab 3-6
  topology 3-10
Router Manager
  exiting 2-4
  introduction 2-1, 3-1
  main window 2-2
  wizards 4-1

S

Safety warning 1-2

Save FRU 2-4
Security
  iSCSI port settings 3-19
  router 3-6
Sensors, MIB B-8
Serial number
  remote router 3-9
  router 3-2
Settings menu 2-4
SNMP
  configuration 3-7
  introduction B-1
  management 3-7
  properties B-1
  trap configuration B-2
  trap receivers 3-8
Software version
  remote router 3-9
  router 3-2
Statistics
  FCIP routes 3-33
  iSCSI ports 3-21
Status 2-3
  FC ports 3-11
  iSCSI ports 3-16
Subnet mask, FCIP routes 3-31
Symbolic name
  remote router 3-9
  router 3-2
System
  contact B-2
  error log messages A-25
  location B-1
  messages A-9
  MIB B-3
System tree 2-3
  window 2-10

T

Target
  iSCSI presented targets 3-27, 3-29
  TCP 3-19
TCP
  max window size, iSCSI ports 3-18
  port number, FCIP routes 3-31
  window scaling, iSCSI ports 3-18
  window size, FCIP routes 3-31
Technical support 1-2
Timeout
  error detect 3-32
  resource allocate 3-32
Timestamp, FCIP routes 3-32
TOE driver
  fatal log messages A-30
  messages A-9
Tool bar 2-7
Topology 3-10
Training 1-3
Trap
  authentication B-2
  community B-1
  receivers 3-8

U

Uni-directional CHAP configuration 5-3, 5-4
Unmap Local Initiator/Target 2-6
Unmap Local Initiator/Target Wizard
  menu option 2-8
  procedures 4-20
Unmap Remote Initiator/Target Wizard 2-6
  menu option 2-9
  procedures 4-40
User modules
  error log messages A-22
  messages A-6

V

Version
  hardware 3-2, 3-9
  software 3-2, 3-9
Vertical tab 3-2

View logs
  icon 2-7
  menu option 2-8
View menu 2-4
VLAN, FCIP routes 3-32

W

Window scaling, FCIP routes 3-31
Windows, system tree 2-10
Wizards
  Add Initiator, launching 2-5
  Add Initiator, using 4-7
  Add Remote Router, launching 2-6
  Add Remote Router, using 4-25
  Configuration, launching 2-5
  Configuration, using 4-2
  Discover iSCSI Target, launching 2-6
  Discover iSCSI Target, using 4-42
  FCIP Route Add, launching 2-6
  FCIP Route Add, using 4-45
  FCIP Route Remove, launching 2-6
  FCIP Route Remove, using 4-51
  FW Update, launching 2-5
  FW Update, using 4-9
  Map Local Initiator/Target, launching 2-6
  Map Local Initiator/Target, using 4-13
  Map Remote Initiator/Target, launching 2-6
  Map Remote Initiator/Target, using 4-33
  menu 2-5
  Remove Remote Router, launching 2-6
  Remove Remote Router, using 4-30
  Unmap Local Initiator/Target, launching 2-6
  Unmap Local Initiator/Target, using 4-20
  Unmap Remote Initiator/Target, launching 2-6
  Unmap Remote Initiator/Target, using 4-40
  using 4-1

Notes